# 序

人类天生就有一种探索周围环境的内在动力，作为年轻人，我和凯文·米特尼克(Kevin　Mitnick)对这个世界有着无比的好奇心并渴望证明自己的能力。我们努力学习新事物、解决难题并赢得比赛，但同时这个世界又告诉我们一个行为规则——不要过于放任自己对探索自由的强烈渴望。可对于最大胆的科学家和企业家，还有像凯文·米特尼克这样的人来说，跟随内心的这种渴望会带来极大的兴奋，并使他们完成别人认为是无法做到的事情。

凯文·米特尼克是我认识的人中最杰出的一个。只要你问他，他便会坦率的告诉你他曾经做过的事——社会工程学——包括骗人。但凯文已经不再是一个社会工程师了，即便在他曾经是的时候，他的动机也绝不是发财和伤害他人。这并不是说这个社会不存在利用社会工程学而给他人带来真正伤害的危险的破坏者，事实上，凯文写这本书的目的就是要提醒大家警惕这些罪犯。

《欺骗的艺术》将会展示政府、企业和我们每一个人，在社会工程师的入侵面前是多么的脆弱和易受攻击。在这个重视信息安全的时代，我们在技术上投入大量的资金来保护我们的计算机网络和数据，而这本书会指出，骗取内部人员的信任和绕过所有技术上的保护是多么的轻而易举。无论你是在政府还是在企业，这本书都如同一个清晰、明确的路标，它将帮助你弄清社会工程师的手段，并且挫败他们的阴谋。

以小说故事的形式展开叙述，不仅有趣，还具有启发性，凯文和合著人比尔·西蒙将把社会工程学这一不为人知的地下世界展现在你的面前。在每个故事叙述之后，他们还将提供一个实用的技术指南来帮助你提防他们在书中所描述的威胁和泄露。

技术上的安全防护会留下很大的漏洞，凯文这样的人可以帮助我们去堵住它。阅读此书，你会发现我们所有的人都终将需要得到“米特尼克”（译者注：指凯文·米特尼克这样的人）的指导。

史蒂夫·沃尼亚克

作者: KEVIN D.MITNICK & William L.Simon

译/王小瑞jroclee[AT＞163.com

前言

一些黑客毁坏别人的文件甚至整个硬盘，他们被称为电脑狂人（crackers）或计算机破坏者（vandals）。另一些新手省去学习技术的麻烦，直接下载黑客工具侵入别人的计算机，这些人被

称为脚本小子（script kiddies）。而真正有着丰富经验和编程技巧的黑客，则开发黑客程序发布到网站或论坛（BBS）。还有一些人对黑客技术没有丝毫兴趣，他们把计算机仅仅当做窃取金钱、商品和服务的辅助工具。

尽管媒体神话了凯文·米特尼克，但我并不是一个用心险恶的黑客，我只是喜欢不断地超越自己。

## 人之初

我的人生之路，也许在我很小的时候就注定了。三岁时，由于父亲的离去，使我无忧无虑的生活发生变故。做招待的母亲支撑着家庭。那时的我（一个由深受没有工作规律之苦的母亲养活着的独生子），除了睡觉以外，大部位时间都没人管，我就是我自己的保姆。

在圣费尔南多谷（San Fernanado Valley）的成长经历给予我探索整个洛杉矶的机会，十二岁时，我发现了一个可以免费周游洛杉矶的方法。我发现到坐公车时购买的换乘劵，是由一种非常规的打孔机打出来的，公车司机用它来在换乘劵上标记日期、时间和路线。一位司机友好地回答了我精心准备的问题，于是我知道了在哪里可以买到这种特殊的打孔机。换乘劵用来改乘车次从而到达目的地，但是我想出的方法，可以让我使用换乘劵免费到达我想去的任何地方。

获得空白换乘劵很容易，如同去公园散步般简单，因为公车终点站的废物箱中总是充斥着公车司机换班时未用完的换乘劵本子。用一叠空白换乘劵加上打孔机，我可以制作出我自己的换乘劵，并用它行遍全洛杉机公车能够到达的任何地方。很快，我就差不多记住了整个公交系统的公车时刻表。（我对某种信息的记忆力总是让人惊讶，这一个较早的例子。直到现在，我还能记住远在童年时的电话号码、口令以及其它一些看上去十分琐碎的事情。）

另一个在小时候就显露出来的个人兴趣是对魔术的迷恋。一旦我知道了某个魔术的变法，我就会不断的练习、练习，再练习，直到我完全掌握。从某种程度上说，正是由于魔术，才让我发现获取秘密信息的乐趣。

## 从盗打电话到黑客

我首次接触社会工程学的时候是在中学时期，那时我遇到了一位喜欢盗打电话的同学。“电话盗打”是一种利用电话公司雇员和电话系统来探测电话网络的黑客行为。他向我展示了使用电话

的高级窍门，比如从电话公司获取任何一位客户的资料，以及使用秘密测试号码拔打免费长途电话。实际上这只是对我们来说免费，因为我后来发现这根本就不是一个秘密测试号码，那些话费事实上从某些倒霉公司的MCI（译者注：美国著名通讯公司）帐户上划出了。

这就是我对社会工程学的入门，也可以说是我的启蒙阶段。我的朋友还有后来认识的另外一个盗打电话的人，他们在给电话公司打电话时让我在旁边听，他们是如何让电话公司相信他们所说的话。于是，我知道了许多电话公司的办公地点，他们的业内用语，还有办公程序。这种“训练”并没有花多长时间，不久我便可以完全自己来做这些事情，甚至比我的启蒙老师们做的还要好。

我生命中下一个15年的生活已经注定。

在中学，我最为喜欢的恶作剧就是获得对电话交换机未授权的访问，然后改变某个电话盗打者的话费设置。当他从家里打电话时，他的电话就会告诉他需要投入一角硬币，因为电话公司交换机的记录被我更改，从而认为他拔打的是一个投币电话。

我开始关注有关电话的任何事情，不只是电子学、交换机和计算机，还有公司组织、业务手续和行业术语。不久之后，我就比任何一个电话公司的雇员都更加了解电话系统。我对社会工程学的运用也达到了娴熟的阶段，十七岁时，我就能与大多数电信公司的员工谈论几乎任何事情，无论是当面聊还是打电话。

实际上我较为公开化的黑客之路，始于中学。尽管在这里我无法说清原委，但其实一句话也能表达了。在我黑客生涯的早期，一个驱使我的动力就是被黑客圈子的人所接受。在那时，黑客这个词是指一个花费大量的时间调置软硬件的人，或是开发更有效的程序，或是绕过不必要的步骤来更快的完成工作。这个词如今已经是一个带有贬义的“恶意犯法者”的意思了，但在本书中，我仍然按原来对它更为善意的理解使用这个词汇。

中学之后，我在洛杉矶计算机学习中心攻读计算机。没几个月的时间，学校的计算机管理人员就意识到我发现了操作系统的漏洞，并取得了管理员权限，但是在学校的教学人员中，最好的计算机专家也无法弄清我是如何这样做的。这也许是最早雇佣黑客的例子之一吧，他们给了我一个无法拒绝的提议：要么做出一个荣誉学位的毕业设计来加强学校的计算机安全，要么由于黑客行为而中止学业。当然，我选择了前者，以本科优等成绩荣誉学士毕业。

## 成为社会工程师

每天早晨，许多人从床上一爬起来，便开始对千篇一律的繁重工作犯愁。我却很幸运，因为我喜欢我的工作。你简直无法想像我作为一个秘密调查者而得到的挑战、奖赏和快乐。我的天份在称为社会工程学（使人们做在通常情况下不会为陌生人做的事情）的表演艺术中得到磨练和回报。

对我来说，成为社会工程学的行家里手并不困难。我父亲家一连好几代都从事销售领域，因此家里人都有着说服和影响别人的家族特征。当把这种特征与骗人的爱好结合起来时，这就是一个社会工程师的基本轮廓了。可以说行骗艺术的分类有两种，一种是通过诈骗、欺骗来获得钱财，这就是通常的骗子。另一种则通过蒙敝、影响、劝导来达到获取信息的目的，这就是社会工程师。从我使用诡计免费乘车的时候（我那时还小，并没有认识到这样做有什么不对），就逐渐意识到我具有一种以前没有料想到的挖掘秘密的天份。通过使用诡计、了解术语和培养良好的操纵技巧，更为加强了这种天份。一个用来发展我的专业技艺（如果这可以称为一个专业的话）的方法就是看我是否能与电话另一端的人攀谈，并获得相关信息，即便这些信息对我毫无用处，这样做只是为了证明我的专业技巧。同样，我还用此种方法，练习奇巧的计谋、托辞，不久我发现我可以取得我想关注的任何信息。正如我在数年后的国会听证会上，在利伯曼（Lieberman）和汤姆森（Tompson）参议员面前所做的证词中描述的那样：

“我未经授权进入了世界上最大的几家公司的计算机系统，并成功渗透了一些防范最好的电脑系统。我使用技术和非技术手段来取得各种操作系统和通讯设备的源代码，以研究它们的漏洞和工作机理。所有的这些行为都是为了满足自己的好奇心。看看自己能做什么，并发现其中的秘密，比如操作系统、移动电话以及任何能引起我好奇心的东西。”

最后的想法

自从被捕以后，我已经承认了自己这些行为的非法，侵犯了他人的秘密。我的错误行为是由于好奇心引起的，我抑制不住的想知道电话网络是如何运转的，以及了解计算机安全的每个细节。我从一个喜欢魔术戏法的孩子成为一个最具恶名的、被政府和企业害怕的黑客。当我反省过去的这30年时，我承认自己做出了极其拙劣的选择，被好奇心驱使，被学习技术的欲望和智力挑战的虚荣所驾驭。

但我现在已经转变，我正在运用我的才能和信息安全、社会工程学的许多有关知识来帮助政府、企业、个人来检测、防范和应对信息安全的威胁。本书可以把我的经验较好地介绍给他人，

以避免那些怀有恶意的信息盗贼可能带来的危害。我相信，你将会从本书中得到乐趣、教育和启发。

内容介绍

本书包含丰富的信息安全与社会工程学的知识，为有助阅览，下面对本书内容做一个简要介绍：

在本书的第一部分（第一章），我将展示信息安全的薄弱环节，并指出为什么你和你们的企业处于社会工程师攻击的危险之下。

本书的第二部分（第二至九章），大家将会看到社会工程师是如何利用人们的信任、乐于助人的愿望和同情心使你上当受骗，从而获得他们想要的信息。本书通过小说故事的形式来叙述典型的攻击案例，给读者演示社会工程师可以戴上许多面具并冒充各种身份。如果你认为自己从来没有遇到过这种事情，你很可能错了。你能从本书的故事中认出自己似曾相识的场景么？你想知道自己是否经历过社会工程学的攻击么？这些都极有可能。但当你看完了第二章到第九章时，便知道下一个社会工程师打来电话时你该如何占取主动了。

接下来的部分将展示一个社会工程师如何铤而走险，进入企业内部，盗取关键信息并越过高级安全防控措施的过程。此部分内容会让人意识到安全威胁存在于各个方面，从普通员工对企业的报复一直到电脑空间的网络恐怖主义。如果你对保持公司业务运转的数据和秘密信息十分重视并为之感到担心，请仔细的阅读本书第三部分（第十至第十四章）。这里需要注明的是：“除非另做声明，本书中的故事情节纯属虚构。”

本书第四部分(第十五至十六章)我将谈到，在业务对话中如何成功的防止社会工程学给企业带来的攻击。第十五章提供一套有效的安全防范培训计划；第十六章也许正解你的燃眉之急——它包含一个完整的安全策略，你可以按公司的需要来立刻应用，以保证企业的信息安全。

最后，本书提供一个由列表、表格组成的“安全一瞥”，用来概括说明一些关键信息，以帮助员工在工作中阻止社会工程学带来的攻击。这些方法还可以为你做出自己的信息安全培训计划提供颇具价值的帮助。

纵览全书，你还可以发现一些非常有用的内容条目：“术语箱”提供社会工程学和计算机黑客的术语；“米特尼克信箱”发出精典短语，有助于加深安全策略的印象；注释与工具条则带来一些有趣的背景知识等附加信息。

# 第一部幕后的故事

## 第一章安全软肋

某公司也许购置了能用钱买到的最好的安全技术，员工们也训练有素，每晚回家前把所有的秘密都锁起来，并从业内最好的保安公司雇用了保安，但这家公司仍然易受攻击。一些人可能遵从了专家所有最好的安全建议，安装了各种受推荐的安全产品，并十分谨慎的处理系统配置以及应用安全补丁，但他们仍然很不安全。

### 人为因素

在国会听证会前的一次证言中，我解释到我经常可以从企业获得密码口令或其他类似的敏感信息，只需假扮某人直接开口要就是了。人们对于绝对安全的渴望常常导致他们满足于虚假的安全感之中。想像一位负责任的可爱的屋主，他有一套麦迪科（译者注：Medico,知名品牌、价格昂贵）防撬锁装在屋子的大门上，以保护他的妻子、孩子和他的家。他觉得很心安，因为他把家庭保护的很好。但对于破窗而入和解开车库大门密码的闯入者呢？再安装一套强壮的安全系统么？虽然有用，但还是不够安全。无论防盗锁是昂贵还是便宜，屋主的安全仍然难以保障。为什么？因为人为因素才是安全的软肋。

安全，通常情况下仅仅是个幻想，由其是轻信、好奇和无知存在的时候。二十世纪最受尊敬的科学家爱因斯坦这样说道：“只有两种事物是无穷尽的——宇宙和人类的愚蠢。但对于前者，我不敢确定。”最终，社会工程学的攻击，成功于人们的愚蠢或更为普遍的对信息安全实践上的无知。

与这位屋主一样，有许多信息技术（IT）从业者都有着类似的错误观念。他们认为自己的公司固若金汤，因为其配置了精良的安全设备——防火墙、入侵检测，或是更为保险的身份认证系统，如时间令牌和生物识别卡。任何认为仅靠这些安全设备即可保证安全的人都会满足于虚假的安全感之中，这就是一个生活在幻想世界中的例子，他们迟早会不可避免的遭遇安全事故。

正如著名的安全顾问布鲁斯·施尼尔（Bruce Schneier）所说：“安全不是一件产品，它是一个过程。”近一步说，安全不是技术问题，它是人和管理的问题。由于开发商不断地创造出更好

的安全科技产品，攻击者利用技术上的漏洞变得越来越困难。于是，越来越多的人转向利用人为因素的手段来进行攻击。穿越人这道防火墙十分容易，只需打一个电话的成本和冒最小的风险。

一个欺骗的经典案例

企业资产安全最大的威胁是什么？很简单，社会工程师。一个无所顾忌的魔术师，用他的左手吸引你的注意，右手窃取你的秘密。他通常十分友善，很会说话，并会让人感到遇上他是件荣幸的事情。我们来看一个社会工程学的例子：

许多人都已记不起一个叫斯坦利·马克·瑞夫金（Stanley Mark Rifkin）的年轻人，和他在洛杉矶的美国保险太平洋银行（Security Pacific National Bank）的冒险小故事了。他的劣迹很多，瑞夫金（同我一样）从未把自己的事情告诉过别人，因此下面的叙述基于公开的报道。

获得密码

1978的一天，瑞夫金无意中来到了美国保险太平洋银行的授权职员准入的电汇交易室，这里每天的转款额达到几十亿美元。瑞夫金当时工作的那家公司恰巧负责开发电汇交易室的数据备份系统，这给了他了解转账程序的机会，包括银行职员拔出账款的步骤。他了解到被授权进行电汇的交易员每天早晨都会收到一个严密保护的密码，用来进行电话转帐交易。

电汇室里的交易员为了记住每天的密码，图省事把密码记到一张纸片上，并把它贴到很容易看得见的地方。11月的一天，瑞夫金有了一个特殊的理由出入电汇室。到达电汇室后，他做了一些操作过程的记录，装做在确定备份系统的正常工作。借此机会偷看纸片上的密码，并用脑子记了下来，几分钟后走出电汇室。瑞夫金后来回忆道：“感觉就像中了大奖”。

转款入户

瑞夫金约在下午3点离开电汇室，径直走到大厦前厅的付费电话旁，塞入一枚硬币，打给电汇室。此时，他改变身份，装扮成一名银行职员——工作于国际部的麦克·汉森（Mike Hansen）。那次对话大概是这样的：

“喂，我是国际部的麦克·汉森。”他对接听电话的小姐说，小姐按正常工作程序让他报上办公电话。“286。”他已有所准备。小姐接着说：“好的，密码是多少？”瑞夫金曾回忆到他那时的“兴奋异常”。“4789”他尽量平静地说出密码。接着他让对方从纽约欧文信托公司（Irving Trust Company）贷一千零二十万美元到瑞士苏黎士某银行（Wozchod Handels Bank），他已经建立好的账户上。对方说：“好的，我知道了，现在请告诉我转账号。”

瑞夫金吓出一身冷汗，这个问题事先没有考虑到，他的骗钱方案出现了纰漏。但他尽量保持自己的角色，十分沉稳，并立刻回答对方：“我看一下，马上给你打过来。”这次，他装扮成电汇室的工作人员，打给银行的另一个部门，拿到帐号后打回电话。对方收到后说：“谢谢。”（在这种情况下说“谢谢”，真是莫大的讽刺。）

成功结束

几天后，瑞夫金乘飞机来到瑞士提取了现金，他拿出八百万通过俄罗斯一家代理处购置了一些钻石，然后把钻石封在腰带里通过了海关，飞回美国。瑞夫金成功的实施了历史上最大的银行劫案，他没有使用武器，甚至勿需计算机的协助。奇怪的是，这一事件以“最大的计算机诈骗案”为名，收录在吉尼斯世界纪录中。斯坦利·瑞夫金用的就是欺骗的艺术，这种技巧和能力我们现在把它称为——社会工程学。

威胁的天然性

瑞夫金的故事确切的证明了我们的安全感是多么不可靠。这样的事件（也许到不了一千万美元，但终归有所损失）每天都在发生，你的资金可能正在流失，新产品方案正在被窃取，而你却一无所知。即使你的公司还没有这样的事情出现，那也会终将出现。但它何时出现呢？

日益增长的安全事件

美国计算机安全协会在2001年计算机犯罪调查报告中声称，在接受调查的组织机构中，有85%的组织在过去的12个月中发现了计算机安全事件。这是一个惊人的数字，只有15%的机构在过去的一年中没有发现安全事件。另一个数字同样惊人，有64%的机构由于计算机的问题而导致财务损失，超过一年中遭受财务损

失企业的二分之一强。

我的经验告诉我这个数字有些夸大，并对这项调查的研究结果表示怀疑。但这并不是说安全事件的危害面不大，相反，它很大。那些未把安全事件考虑在内的人，迟早会出问题。大多数公司配置的安全产品主是应付业余入侵者的，比如被称为“脚本小子”的年轻人。实际上，这些利用别人的软件，并憧憬着成为真正黑客的人，大多数情况下只能引起一些麻烦。真正的损失和威胁，来自于经验丰富、目标清晰，受商业利益驱动的攻击者。这些人一次只盯准一个目标，而不像业余入侵者试图进入尽可能多的系统。业余黑客看重数量，而职业黑客在乎的是信息的质量和价值。

认证设备（身份认证）、访问控制（对文件和系统资源的控制管理）和入侵检测系统（计算机化的防盗器）等技术，对公司的安全防护是十分必要的。然而，现在的公司在布置保护企业免受攻击的安全对策方面的投入比其花在咖啡上的钱还要少。

正如同罪恶的心无法抵制诱惑，黑客们一心要找出功能强大的安全系统的弱点。在许多时候，他们把这种心思放在了人的身上。

欺骗的使用

许多人都说，关掉了的计算机才是安全的计算机，但这是错误的，找个借口让人去办公室打开它就是了。你的对手不仅仅有一种方法可以从你那里得到他想要的信息，这只是时间的问题。耐心、个性和坚持，这正是欺骗的艺术的切入点。

要击败安全措施，一个攻击者、入侵者，或是社会工程师，必须找到一个方法，从可信用户那里骗取信息，或是不露痕迹的获得访问权。当可信用户被欺骗、影响，并被操纵而吐露出敏感信息时，或是做出了不当的举动，从而让攻击者有漏洞可钻时，什么样的安全技术也无法保护住你的业务了。正如同密码专家有时通过寻找漏洞来绕过加密技术解出密文一样，社会工程师通过欺骗你的雇员来绕过安全技术。

信任的弊端

大多数情况下，成功的社会工程师都有着很强的人际交往能

力。他们有魅力、讲礼貌、讨人喜欢，并具有快速建立起可亲、可信感的特点。一个经验丰富的社会工程师，使用他自已的战略、战术，几乎能够接近任何他感兴趣的信息。精干的技术专家辛辛苦苦地设计出安全解决方案来最小化使用计算机的风险，然而却没有解决最大的漏洞——人为因素。尽管我们很聪明，但对我们人类——你、我、他的安全最严重的威胁，来自于我们彼此之间。

我们的国民性格

我们对危险漠不关心，尤其在西方，美国则更甚。我们没有受到要对别人保有怀疑态度的训练，我们接受的是“爱汝之邻”（译者注：此句引自《圣经》）的教育，人与人之间要相互信任和忠实，试想一下小区的保安机构让人们锁上家门和车门是多么的困难。这种情形是很明显的，却似乎被许多宁愿活在理想世界里的人忽略，直至受到伤害。

我们知道，并不是所有的人都诚实善良、友爱可亲，可我们在生活中却经常把他人想像成这样。这种可爱的无知一直都是美国人的生活方式，放弃这种习惯十分不易。做为美国人，自由和最适宜居住的地方就是锁和钥匙最没必要的地方，这种理念已经深入人心。大多数人持有不会被欺骗的想法是觉得被骗的可能性很低，而攻击者利用这种心理，编出不会引起怀疑的听上去十分合理的理由，充分的利用了受骗者的信任。

机构的无知

无知是我们国民性格的一部分，这可以在回溯计算机首次远程联接时轻易的看出。APPANet（美国国防部高级研究项目署网络），互联网的前身，用来在政府、科研和教育机构之间共享信息，其目标是信息共享和科技进步，许多教育机构因此建立了几乎没有任何安全措施的早期计算机系统。一个著名的软件开发自由主义者，理查德·斯托曼，甚至拒绝为他的账号设置口令。但随着互联网电子商务的兴起，由于互联网脆弱的安全措施导致的危害性发生了极大的变化。

使用再多的安全技术也不能解决人为的安全因素，拿今天的机场为例，安全已经成为首要措施，然而我们仍然被媒体的报道所警告，还是有人可以避开安全措施、携带潜在性武器通过检测。在一个机场时刻处于警戒状态下的时期，这种事情又是怎么

发生的呢？是那些金属仪器失效了么？不，问题不在机器，问题在于人，机器是由人操纵的。机场的官员虽然可以布署国民警卫队并安装检测器和面部识别系统，但如何培训一线保卫人员正确地检查旅客则更为重要。全世界的政府、商业、教育机构都有同样的问题，虽然各个地方的职业安全人员不敢懈怠，但信息仍然易受攻击，并被具备社会工程学技巧的攻击者视为可摘之果，除非安全链中最薄弱的环节——人为因素，被加固强化。

现在，我们比任何时候都需要停止幻想，同时对攻击计算机系统和网络机密性、完整性以及实用性的技术加深认识。我们已经认识到主动防御的必要，是接受和学习安全防护的时候了。

对你的隐私、思想和公司信息系统的非法入侵似乎很遥远，直到它真的发生。为了避免付出昂贵的代价，我们所有的人都需加深认识、富有经验、保持警醒，并主动防卫我们的信息资产、个人信息，以及国家的关健基础设施。现在，我们必须实行严谨、周密的设防。

欺骗与恐怖分子

当然，欺骗并不是社会工程师的专用工具。暴戾的恐怖主义制造了耸人听闻的新闻事件，我们前所未有地意识到我们居住的世界充满了危险。文明，终归只是一层脆弱的薄板。2001年，发生在纽约的911事件把悲伤和恐惧植入每一个人的心中，不只是美国人，还有世界上所有善良的人们。我们已经开始警觉，因为这个世界上还分布着受到良好训练的极端恐怖分子，伺机再次发动对我们的攻击。

政府最近的强化努力已经提升了大众的安全意识，我们需要保持警醒，警惕各种形式的恐怖主义。我们需要了解恐怖分子是如何伪造各种身份，假扮学生、邻居而混入人群的，他们掩饰住自己真实的思想以密谋恐怖行动，而他们使用的就是类似于本书中介绍的欺骗手法。

然而，就我所认为，恐怖分子目前尚未利用社会工程学的手法渗透到水处理厂、发电厂，或其它关系国计民生的基础设施中，但可能性依然存在，这毕竟太容易做到了。我希望安全意识和相应的安全策略将会得到正确的应用并得到企业上层管理的加强，因为这本书恰逢其时。

关于此书

企业安全是一个平衡问题，安全性太差公司易受攻击，但过多的强调安全又会妨碍业务管理和公司的发展，其难点在于达到生产效率和安全之间的平衡。

其它关于企业信息安全的书都把重点放在硬、软件技术上，而忽略了最重要的安全威胁——对人的欺骗。与之相反，此书的目的，就是要帮助大家理解自己、同事，和公司其他人员是如何被操纵的，并帮助大家建立屏障，谨防成为受害者。本书的重点放在入侵者用来盗取信息的非技术手段上，它能够对看似安全的信息完整性产生威胁，甚至破坏公司的工作成果。

我的任务由于一个简单的事实而更加困难——每个读者都一直被社会工程学高级专家——他们的父母所控制着，他们有办法（比如："这是为了你好"）让你去做他们认为最应该做的事。父母们就是使用类似社会工程学的方法，巧妙的编出看似有理的故事、理由以及借口，来达到他们的目的。是的，我们都被我们的父母所引导——那些乐善好施的（偶尔也不完全如此）社会工程师们。

由于这种生长环境，导致我们软弱而容易被操纵。可总是对他人怀有戒心，担心上当受骗，会活得很累。在理想的世界里我们应对他人给予绝对信任，每个人都是诚实和值得信赖的。但我们并没有生活在理想世界中，我们必须锻炼我们的防欺诈能力以对付我们的敌人。

这本书的主要内容——第二和第三部分，讲述社会工程师如何实施欺骗的故事。在这两部分中，大家将会看到如下内容：

·电话盗打者早就发现的，一个从电话公司弄到未刊登电话号码的方法；
·几个不同的社会工程学方法，甚至可以让有所警觉和怀疑的职员吐露出自己的用户名和口令；
·信息中心的管理人员如何被控制以配合攻击者窃取企业最机密的产品信息；
·隐私调查者是如何弄到你的企业、你本人的隐密信息的，我可以保证，这会让你脊背发凉。

你也许会认为这两部分中讲述的故事实际上不可能发生，没有人能够使用书中的谎言、卑鄙的方法和计划真正的达到目的。

事实上，在每个案例中，这些故事都是可以成为现实而且已经成为现实的，这些事情每天都在世界的某个地方发生，甚至在你阅读此书的时候都有可能。本书中的内容不仅对你的商务信息保护上有所启迪，还可以让你亲自阻挠社会工程师的攻击以保护你的私有信息。

在本书的第四部分，我转变了方向。在这里我想帮助大家建立企业必要的安全策略和安全意识培训，以期将员工被社会工程师利用的可能性降到最低。了解社会工程师的策略、方法和技巧，在不会降低公司的生产效率的同时，帮助你布置合理的控制策略来保护企业的信息资产。

简而言之，我写此书的目的就是要提升大家的安全意识，以应对来自社会工程师的严重威胁，并帮助你的公司和公司员工尽可能的不被利用。或者我应该这样说，不再被利用。

## 第二部攻击者的手段

### 第二章无害信息的价值

对大多数人来说，社会工程师的真正威胁在哪里？又该如何保持警惕？

如果社会工程师的目标是“最有价值奖”——比如，企业智力资产的核心组成。那么也许需要的是更坚固的保险库和全副武装的保安，对么？

但在现实中，坏人渗透企业安全的第一步就是获得某些似乎无利害关系的信息和文件，这些信息和文件看起来十分平常，也不重要，公司里的人大都不明白为什么这些东西会被限制和保护。

#### 信息的隐藏价值

社会工程师十分重视企业中许多表面上看去无利害关系的信息，因为这些信息是他能否披上可信外衣的至关重要的因素。

在这一章里，我将通过让读者“亲身”经历攻击过程，来展示社会工程师的攻击手段。有时从受害人的角度来表现情节，让读者以当事人的身份估计自己（或是你的同事和员工）可能会做出的反应。而更多的时候，让读者从社会工程师的角度来经历攻击过程。

第一个故事着眼于金融行业的一个漏洞。

#### 信誉支票(CREDITCHEX)

曾经有一段很长的时期，英国的银行系统十分闭塞，大街上一位诚实普通的市民并不能随便走进银行而直接申请一个银行帐户。银行不会把他当做客户，除非他带有某位正式银行客户的推荐信。

当然，这与如今的表面上人人平等的银行机构大不一样。如今办理银行业务没什么地方比友善、平等的美国更方便了，任何人都可以走进银行轻松的建立一个日常账户，是这样么？

并非如此。事实上可以理解，银行很难为一个才开过空头支

票的人建立账户，这很自然，同样还有那些有着抢劫银行和挪用账款记录的人。这就是一个银行对其潜在客户瞬间做出好坏判断的实际例子。

与银行有着重要业务联系的公司中，有一种机构专门为银行提供这类信息，我们把这种机构称之为“信誉支票”。它为客户提优质的服务，但同许多公司一样，它也会“无心”的为“有心”的社会工程师们提供便利的服务。

第一个电话：吉姆·安德鲁斯(Kim Andrews)

“国家银行，我是吉姆，您是想要开一个帐户么？”

“嗨，吉姆，我想请教个问题。你们与信誉支票打交道么？”

“是的。”

“你们给信誉支票打电话时，怎么称呼你们提供的号码？是叫‘交易号’(Merchant ID)么？”短暂的沉默，基姆在衡量这个问题，对方是什么意图，她是否应该回答。打电话的人不容对方思考接着问：“是这样，吉姆，我在写一本涉及私人调查的书。”

“是的。”她有了回答的信心，因为她还是愿意帮助一个作家的。

“就叫“交易号”，对么？”

“啊，嗯。”

“好的，很好。我是想确认我的书中使用了正确的专业用语，谢谢你的帮忙，再见，吉姆。”

第二个电话：克瑞丝·塔伯特(Chris Talbert)

“国家银行，开户处，我是克瑞丝。”

“嗨，克瑞丝，我是阿莱克斯。”打电话的人说，“我是‘信誉支票’的客服代表，我们在做一项改善服务质量的调查。能耽误您几分钟么？”克瑞丝表示愿意，打电话的人继续：“好的。你们部门营业时间是多少？”她给予回答，并接着回答下面的一系列问题。

“你们部门有多少人使用我们的服务？”

“大约多长时间给我们打一次咨询电话？”

“您用的是我们哪一个800免费电话号码？”

“我们的客服代表服务态度好么？”

“我们对业务的响应时间如何？”

“您在银行工作多长时间了？”

“您通常使用的交易号是多少？”

“您是否发现过我们提供过的信息不准确？”
“如果您对我们的服务有所建议，建议是什么呢？”最后：
“如果我们把定期调查表寄到你们部门，您会填写么？”

她表示同意，然后彼此简单对了几句话，电话挂掉，克瑞丝继续她的工作。
第三个电话：亨利·麦克金赛(Henry McKinsey)

“信誉支票，我是亨利·麦克金赛，需要帮忙么？”

打电话的人表明自己是国家银行的职员，并报出正确的交易号，以及他想查询的人的名字和社会保险号。亨利要求出生日期，他也报上。不一会儿，亨利看着自己的计算机屏幕读道：“韦尔斯·法果在1998年报过一次NSF”——客户账款不足（Non Sufficient Funds），支票已开出，账户里却没有足够钱支付的银行常用专业用语。

“自那之后，还有资金往来么？”
“没有了。”
“有没有申请其他账户？”
“我看一下。有的，两次，都在上个月。一次是在芝加哥第三联合信用会（Third United Credit Union of Chicago），”他断断续续地读出第二个地方，斯卡奈塔第共同投资（Schenectady Mutual Investments），他不得不逐字母的将名称拼出。“纽约州。”他最后补充道。

工作中的私人侦探

所有的这三个电话都是同一个人打的，一个私人侦探，我们且称他为奥斯卡·格瑞斯（Oscar Grace）吧。格瑞斯有了一位新客户，他的首批客户其中之一。几个月前还是名警察的格瑞斯发现他的新工作有些做起来易如反掌，有些则对他的智力和创造性是个挑战，这件案子无疑很具有挑战性。

小说中的冷面神探——塞姆·斯贝兹（Sam Spades）和菲利浦·马洛斯（Philip Marlowes），在漫长的夜晚久候在汽车里诱捕一位骗人的伴侣（译者注：塞姆和菲利浦都是著名小说和电影中的人物），现实中的私人侦探也做同样的事情。他们为相互敌对的伴侣之间打探消息，也许没小说中写得那么夸张，但重要性却一点不差。他们的方法主要是依靠社会工程学的技巧，而不是坐在

车子里与守夜的困倦做斗争。

格瑞斯的新客户是一位看起来从不缺少衣服和珠宝的女士。一天，她走进他的办公室，在唯一的一把未堆着文件的皮椅上坐下来，把她的古琦（译者注：Gucci，意大利名牌）手包放到桌子上，商标冲着他的脸。这位女士告诉格瑞斯，她想跟他的丈夫离婚，但“有一点小麻烦。”

他的丈夫比她早了一步，已经从两人的储蓄帐户中把存款提了出来，并从代理公司（译者注：专门从事为客户买卖股票和债券的公司）的账户中提走了更大的款项。她想知道他们的钱到哪里去了，她的离婚律师对此无能为力。格瑞斯猜想她的律师是那种身居住宅区高楼大厦的法律顾问，才不会为这种“钱到哪里去了”的烂事自找麻烦。

格瑞斯有办法么？

他向她保证这是小事一桩，接着报出价格，列出费用，并收了一张支票做为第一笔佣金。接下来，他要面对此事了。如果你以前从未处理过这样的事情，并根本不知道如何跟踪一笔资金的来龙去脉，你该从何做起呢？一步一步地往前挪？好吧，我们来讲格瑞斯的故事。

我知道信誉支票以及银行与其的联系，我的前妻曾在银行工作。但我并不知道那些专业术语和业务过程，而向我前妻打听则是浪费时间。

第一步：了解专业术语，设计出获取信息时所需要的对话，以便听起来不会露出马脚。我给银行打电话时，第一位年轻的小姐，吉姆，在我询问他们如何向信誉支票确定自己身份时就有所迟疑，她犹豫着，不知道是否应该告诉我。我被难住了么？才不。事实上，她的犹豫给了我一个重要的线索，提醒我必须给她提供一个可信的理由。当我骗她说为写一本书而做的调查时，便打消了她的怀疑。声称自己是一位作家或电影剧本作者，可以让人放松警惕。

她知道一些有用的信息，比如信誉支票如何确定打电话人的身份，你可以查询哪些信息，最重要的——吉姆所在银行的交易号。我已准备好提出这些问题，但她的犹豫造成了麻烦。吉姆相信了写书的故事，可她已经有所疑心。如果她更配合些，我就会

多问些操作细节了。

专业术语

马克（MARK）：受骗者

激警（BURN THE SOURCE）：攻击者如果让对方看出来攻击的意图称为激警。一旦对方有所警觉并通知其他人员，以后再想套出类似的信息就十分困难了。

你必须依靠自己的感觉，仔细的倾听马克的说话内容和说话方式。这位小姐看起来就十分聪明，如果我提出很多的敏感问题，她一定会敲响警钟的。即使她不知道我是谁，我用哪个号码打过来，也不要让任何人注意到有人在打探消息而有所警觉。这是因为我们不想激警，有可能还需要给这个地方打电话的。

我总是留意那些能够帮助我了解一个人配合程度的微小迹象，其态度各异，从“你听起来真是一个好人，我相信你所说的每一句话”到“打电话给警察，通知国民警卫队，这小子要倒霉了。”

我发现了吉姆的警觉，于是我打电话给另一个人——克瑞丝。在我的第二个电话中，调查表的把戏很能迷惑人。我把重要的问题插进可以建立信任感的无关紧要的问题中，在信誉支票的交易号问题之前，我通过问她在这家银行工作多久了这样一个私人问题，做了一个最后的小测试。

私人问题就像一颗地雷，有些人会毫不注意的踩上去，有些人则知道它会爆炸，赶紧躲开。因此，如果我问及一个私人问题，她在回答的语气上没有变化，这就意味着她很可能没有对提问产生怀疑，我可以在她没有疑心的问题之下安全地提出关健问题。

一个好的私人侦探还知道，千万不要在得到关键信息后马上结束谈话。多问两三个问题，小聊一会儿，然后再说拜拜。如果对方稍后想起你提过的问题，很可能是你最后提出的问题，其它的通常会忘记。

这样，我从克瑞丝那里得到了他们的交易号和他们查询时所用的电话号码，如果当时我再多问些信誉支票的事，我会更高兴的。但没有进一步冒险，也许更好。

如同有了一张空白支票，无论什么时候我都可以从信誉支票

那里获得我需要的信息，甚至不用付费。从前面的情况看出，信誉支票的客服代表十分愿意为我提供信息，于是我知道了我客户的丈夫最近在两个地方申请建立账户。那他将要离婚的妻子寻找的那笔资产在哪里呢？无论在哪家银行，信誉支票都会将其列出吧？

过程分析

整个过程都基于社会工程师的基本策略之一，获得公司职员认为无关紧要的信息（实际上它是有用的）。第一个银行职员肯定了打电话给信誉支票时确认身份的术语，第二个职员提供了电话号码和最至关重要的信息——交易号。透露这些信息对于她们来说似乎是无所谓的，毕竟她们认为与之交谈的是信誉支票的工作人员，把号码说出来又有什么不对呢？

前两个电话为第三个电话打下基础，格瑞斯已经具备给信誉支票打电话需要知道的一切信息，于是冒充信誉支票的客户——国家银行，轻松地查询信息。

格瑞斯窃取信息的技巧丝毫不逊于一个高超的骗子诈骗钱财时所用的手段，在了解人方面格瑞斯久经磨练。他懂得把关键信息藏在无关紧要的信息中，也知道在套出交易号之前用私人问题来测试对方的配合程度。

第一个银行职员在确认信誉支票专业术语上的错误几乎是最难防范的，这种专业用语在银行业几乎人人都知道，因此显得无关紧要——无害信息最普遍的表现形式。但第二个职员，克瑞丝，不应该在确定打电话人的身份真实与否之前，就非常乐意的回答问题。她至少应该询问对方的名字和电话号码并拔回，这样如果日后发生问题，她还有一个打电话人所使用电话号码的记录。在这个案例中，拔回这样的一个电话还会给攻击者假扮信誉支票服务人员造成很大的困难。

米特尼克信箱

这个案例中的交易号相当于一个密码，如果银行工作人员将其与自动取款机的个人识别码（PIN）一样看待，便会对它的敏感性给予重视。你所在的机构中有没有大家没有给予重视的编码和数字呢？

用以前记录的银行电话号码给信誉支票回拨一个电话（不要用对方提供的号码），以验证对方是否在那儿工作，信誉支票是否正在做一项客户调查，这样的电话还是有必要打的。现代社会人们的工作时间都很紧张，而且这样的确认电话会占用不少时间，考虑到现实中的实用性，建议工作人员在对对方的目的性有所怀疑时打回一个确认电话。

工程师的圈套

很多人都知道，猎头公司使用社会工程学来扩大业务范围，这里有一个例子：

在90年代末，某个不怎么道德的职业介绍所签了一家新客户，一家正在寻找有通讯行业工作经验的电气工程师的公司。负责这个项目的经理是一位女士，有着有磁性的嗓音，和充满诱惑力的言谈举止，这使得她在电话里很容易获取别人的好感和信任。这位女士准备对移动电话服务提供商进行一次偷袭，以期找到一些可能会投奔到竞争对手那里的工程师。她当然不能直接给接线员打电话说："我要找五年经验的工程师"，那样她的动机会立刻暴露的。她通过询问看上去无关紧要的信息，电话公司人人都可以告诉别人的信息，巧妙的发动了这次袭击。

第一个电话：接线员

攻击者使用迪迪·桑德斯这个名字给移动电话服务商的总机打了一个电话，对话情形大致如下：

接线员：下午好，我是玛丽，您有什么事情？
迪迪：请帮我接运输部好么？

接：我不一定能找到这个号码，我查一下目录，您是哪位？
迪：我是迪迪。
接：您在公司大楼里还是在……？
迪：不，我在外面。
接：你是迪迪……？
迪：迪迪·桑德斯，我以前知道运输部的分机号，但我现在忘了。
接：稍等。

为了减少怀疑，在这里迪迪设计了一次谈话，让对方认为她

是内部人员，熟悉公司的情况。

接：您在哪里办公？主街商厦（Main Place）还是望湖大厦（Lakeview）？

迪：主街。（停顿一下）接：电话是805-555-6469。

有可能给运输部打电话后也得不到所需的信息，迪迪又要了资产部的电话，作为备用。接线员帮迪迪接到运输部，但线路正忙。于是，迪迪又问第三个电话，位于得克萨斯州首府奥斯丁的收款部号码。接线员让她等一会儿，并放下电话。接线员有所警觉了么？她在向保卫部门报告她接到一个可疑电话么？才不，迪迪一点都不担心。接线员只是有些不耐烦了，但这是她再平常不过的日常工作了。一分钟后，接线员拿起电话，查到收款部的号码，给迪迪接通。

第二个电话：派基（Peggy）

对话大致如下：

派基：收款部，我是派基。

迪迪：嗨，派基，我是橡木城（Thousand Oaks）的迪迪。

派：嗨，迪迪。

迪：你好吗？

派：还好。

迪迪接着使用企业内部的习惯用语来描述成本核算代码——给一个特定的机构或工作组分配费用的代码（译者注：常在报销费用时填写）。

迪：很好。我有个问题问你。我如何才能找到某个部门的成本中心（cost center）？

派：你必须联系到那个部门的预算师。

迪：你知道谁是橡木城总部的预算师么？我在填表，但我不知道该填哪个成本中心？

派：我只知道要找成本中心的代码时，打电话给预算师。

迪：你们部门在德克萨斯有成本中心么？

派：我们有自己的成本中心，但我们没有完整的成本中心列表。

迪：成本中心的代码是多少位？比如，你们的成本中心？

派：嗯，这样，你是9WC还是SAT？

迪迪并不知道这是指哪个部门或工作组，但这并不重要，她回答道：

迪：9WC。
派：那一般是四位数字。你说你在哪里？
迪：橡木城总部。
派：哦，这里有橡木城的代码。 1A5N，N是Nancy的N。

仅仅与愿意帮忙的人打交道到足够时间，迪迪便得到了她需要的代码，这个代码就是所谓的被人认为是无需保护的信息，因为它对企业外面的人来讲，似乎没有任何价值。

第三个电话：有用的错误号码

迪迪的下一步是把成本中心的代码当做筹码来开发更大的价值。她先给资产部打电话，假装是故意拔错的电话。以“不好意思，但……”做为话头，她声称自己丢失了公司的通讯录，看看对方可不可以帮她弄一个新的。对方说公司已将通讯录放在内部网站上，打印出来的已经过期了。迪迪说她还是想要一份复印件，对方让她打刊印部的电话，并主动查到刊印部的电话（也许是想让这位声音性感的女士多在电话上呆一会儿吧）然后告诉了她。

第四个电话：刊印部的巴特

在刊印部，她与一个叫巴特的人谈上了话。迪迪说她是橡木城的，他们新来了一位顾问，需要一份公司的通讯录。她告诉巴特，对于这位顾问来说，一份复印件会让工作更顺利些，即便有些过期。巴特告诉她需要填一份申请单然后再寄给他。迪迪说她手头没有申请单，而且事情很急，她甜言蜜语地问巴特是否能发个善心帮她填这个单子？他有些过分热心地同意了，接着迪迪报出单子上的各项内容。在报出虚构的签单人地址时，她慢慢地说出了一个被社会工程师称为“秘密通信地”的号码，在这里是一个邮箱号，商用的，她的公司为类似这种情况而租用的邮箱。这时，早先的准备工作派上了用场。邮递这份目录会产生费用，迪迪给出了橡木城成本中心的成本核算代码：“1A5N，N是Nancy的N。”

几天后，企业通讯录寄到，迪迪发现比她期望的还要好。上面不仅有名字和电话号码，还有人员之间的工作关系，整个企业的组织结构。

这位有着磁性嗓音的女士可以通过拔打人员电话开始她的猎头行动了。她使用社会工程师久经磨练的谈话技巧，骗取了开始行动所需的信息，她现在已经准备好收获了。

专业术语

秘密通信地（Mail Drop）：社会工程师把租来的邮箱称为秘密通信地，通常是用假名字租用的，用来接收受骗者发来的文件和包裹。

米特尼克信箱

犹如拼图游戏，每条信息本身并没有什么联系。然而，当把它们放在一起时，一个清晰的画面便出现了。在这个案例中，社会工程师看到的画面就是那家公司的整个内部结构。

过程分析

在这次社会工程学的攻击中，迪迪以获得目标企业的三个部门电话为开始。这很容易，因为她询问的电话号码并不是秘密，尤其是对于内部工作人员。一个社会工程师要听起来像一个内部人员，此例中的迪迪就很善此道。一个电话号码帮她弄到成本中心的核算代码，而后者用来获取公司职员的通讯录。她使用的主要工具是：友善的语气、企业专业用语，以及对那个最后的上当者抛一个口头上的媚眼。还有一件无法轻易得到的必不可少的工具——社会工程师的操纵能力，它来自于广泛的实践，和老一辈骗子们口头传下来的经验。

更多的“无价值”信息

除了成本核算代码和内部分机电话，还有哪些看似无用但对你的敌人来说非常有价值的信息？

皮特·艾伯尔（Peter Abel）的电话

“嗨，”电话的另一端说：“我是帕克斯特（Parkhurst）旅行社的汤姆，您去往旧金山的机票已订好，您要寄过去还是您来拿？”

“旧金山？”皮特说：“我没打算去旧金山。”

“您是皮特·艾伯尔么？”

“是的，但我没有任何旅行的安排。”
“嗯，”对方友好的笑笑，“您确定您不想去旧金山么？”
“如果你认为你能跟我老板谈谈此事的话……”皮特对这次友好的谈话开起玩笑。
“这听起来有些乱，”对方说：“我们的系统依照员工号码登记旅行安排，也许有人把号码弄错了，你的员工号码是多少？”

皮特欣然报出他的号码。为什么？因为这如同他平时所填的公司里很多人都会看到的人员登记表，人事部、工资名单，很明显，还有外面的旅行社。没人把员工号码当做秘密。这会有什么影响吗？

这很难说清。两到三个信息也许就可以让社会工程师装扮成他人扮演一场好戏了。弄到一个工作人员的名字和他的电话号码，也许为了保险起见，再找到他上司的名字和电话号码。即使一个不怎么出色的社会工程师也会尽可能的搜集所需要的信息，以使他给下一个目标打电话时听起来可信。

如果昨天有人给你打过电话，声称他是公司另一个部门的职员，并给出一个含糊的理由来询问你的员工号码，你很轻易的就告诉他了么？

还有，你的社会保险号呢？（译者注：美国、加拿大居民的身份代码，类似于中国的身份证号。）

米特尼克信箱

这个故事的寓意在于，不要把任何个人和公司内部信息或是识别标识告诉他人，除非你听出她或他的声音是熟人，并确认对方有这些信息的知情权。

预防措施

公司有责任让员工意识到对非公共信息的管理不善会带来严重的后果。一个深思熟虑地信息安全策略，再加上正确的教育和培训，将会极大的提升员工正确处理企业内部信息的意识。资料数据的分类策略也将帮助你实施对信息使用的正确控制，如果没有分类策略，所有的内部信息都应被视为保密，除非另做指定。

采取以下步骤来防止公司看似无害信息的泄漏：

信息安全部门应操办意识培训来讲解社会工程师所使用的手段。其中一个方法，正如上文所提到的，就是获得看似不敏感的信息，然后把它当做筹码来取得短暂的信任。每一个员工都应该意识到，当一个知道公司办事程序、专业用语和内部标识的人打来电话时，并不意味着他或她就可以知道所查询的信息。对方可能是公司以前的员工或是知道公司内部一般情况的合同工（译者注：某些大公司将员工分为regular和contractor，前者类似事业单位的固定工，后者类似合同工）。因此，每个企业都有责任制定适当的验证方法，在员工与他们不认识的人通电话或当面交谈时使用。

负责制订资料分类政策的人应该仔细检查信息的分类，注意那些正式员工可以访问到的看似无害却可能会导致敏感信息泄漏的信息。尽管你从未把现金卡（ATM）的密码告诉过别人，但你曾把开发公司软件产品的服务器告诉过别人么？这个信息可不可以让一个人装扮成企业员工合法地访问企业网络呢？

有时仅仅知道内部的专用术语，就可以让社会工程师显得知道很多并可以信赖，攻击者常常利用这个普遍的错误观念来操纵受骗者。比如，交易码是银行开户处用工作人员每天都使用的认证标识，这个标识的意义与密码一模一样。如果每一个工作人员都认识到它的意义——唯一用来确认查询人身份，他们也许会更加谨慎的对待它。

米特尼克信箱

正如人所说——即使一个真正的妄想狂也可能有敌人，我们也必须假定每个企业都有它的敌人——以网络设施为目标危及商业秘密的攻击者。不要只把计算机犯罪视作一个统计数字，应尽早地布置深思熟虑的安全操作方案和策略，这样才能对企业进行正确的控制以加强防范。

没有公司或只有很少的公司，会将首席执行官或董事长的直拨电话告诉别人。尽管大多数公司并不在意在内部公开电话号码，尤其对于似乎是内部员工的人，实施这样一个政策还是必要的：禁止对外公开内部职员、合同工、顾问和临时雇员的电话号码。

部门或工作组的财务制度，还有企业通讯录（无论是复印件还是资料文件或是内网上的电子版），都是社会工程师常见的目标。每个企业对这类信息都要有一个成文的使用政策，并让所有的员工都知道。保安人员则应保留一份备查日志，用以记录敏感信息透露给企业外人员的情况。像员工号码这样的信息，它本身不能用做任何形式的验证，内部员工不仅要验证查询信息者的身份，还要确定对方是否具有相关信息的知情权。

在进行安全培训时，试一下这个方法：无论什么时候在接受一个陌生人询问时，首先要礼貌的拒绝，直到确认对方身份。然后，在做好心人之前，先遵循公司对非公共信息的验证和使用政策。这种工作方式也许违背了我们乐于助人的天性，但多一点有益的怀疑也许是必要的，以免成为社会工程师的下一个受骗者。

正如本章故事中所叙述的，看似无害的信息也许会成为打开企业最有价值的秘密信息的钥匙。

## 第三章正面攻击——直接索取

很多时候，社会工程学的攻击是十分复杂的，包括一系列的步骤和精心的策划，并同时具备操作技巧和透彻的背景知识。但令人惊奇的是一位技艺高超的社会工程师经常可以使用简单、直接、正面的攻击方式来达到目标。直接了当的开口要求所需的信息，也许仅此一点就已经足够，正如下文中你即将看到的。

### 快速搞定线路分配中心

想知道某人未登记的电话号码么？一个社会工程师可以告诉你半打的方法（你也可以在本书中的其它故事内容中看到），但最简单的办法就是拨出这样的一个电话……

### 请告诉我号码

攻击者拨打线路分配中心（Mechanized Line Assignment Center）未公开的电话公司号码，接听电话的是个女子，攻击者说道："嗨，我是保罗·安东尼（Paul Anthony），我是线路员。是这样，这里有一个接线盒在火灾中烧毁，警察认为是有人故意烧掉自己的房子来骗保险。他们让我一个人来为二百对接线柱接线。现在，我真得需要帮忙了。南大街6723号的线路是怎样分配的？"

电话公司的人都知道，对于非公开的号码查询信息只能让已授权的电话公司知道，线路分配中心的的号码只能告诉本公司的职员。然而，即使他们从不会将这些信息公之于众，谁又能拒绝帮助一位身负繁重工作任务的公司员工呢？她对他保罗起了同情之心，她今天的工作也很不顺，于是她小小地破了个例，来帮助这个遇到麻烦的同事。她告诉他电缆线的配对，以及每个分配到相应地址的号码。

### 米特尼克信箱

人们都很容易相信自己的同事，尤其是在其要求满足合理的测试之后。社会工程师便利用这种知识从受骗者身上获取信息以达到他们的目标。

### 过程分析

正如你不断地在这些故事中看到的，企业专业术语的知识和它的结构组织——各个办公室和部门都是做什么的、具备什么样的信息，是一个优秀社会工程师的骗术箱中的必备品。

逃亡者

一个我们将称之为弗兰克·帕森斯（Frank Parsons）的人已经在逃多年，作为60年代地下反战组织的一分子，他仍然被联邦政府通辑。在餐馆里，他总面对着门口坐着，习惯于左顾右盼，偶尔会被人注意到神色紧张。

弗兰克每隔几年都会搬家。有一次，他来到一个陌生的城市，准备找个工作。对于弗兰克这样有着精湛计算机技术的人（同样，还有娴熟的社会工程学技术，即便他从不会把这写到应聘简历上），找到一个不错的工作还是很容易的。只要不是处于经济特别紧张的时期，具备良好计算机知识的人很容易得到施展才能的机会并摆脱困境。弗兰克很快的看中了一份薪资优厚的工作，一家庞大、高级的长期疗养院，而且离他住的地方很近。

他想，这真合适。但当他埋头苦干地填写申请表时，忽然碰到一个麻烦。雇用方要求应聘者提供一份犯罪历史记录的复印件，这份复印件他只能亲自去州警察局去拿。在工作申请表里就包含着一张需要这个复印件的表格，上面还有一个用来按指纹的地方。即便他们只需要右手食指的指纹，但如果把这个指纹与联邦调查局数据库中的指纹做比较的话，他可能很快就要到联邦政府资助的地方（译者注：指监狱）食堂工作了。

另一方面，对于弗兰克来说，还可能（仅仅是可能），仍然平安无事，州警察局也许根本不会把指纹样发到联邦调查局。但他如何获知这一点呢？

怎么办？他是一个社会工程师，你认为他会怎么做呢？

弗兰克往州警察局拨了一个电话：“嗨，我们正在为州司法部执手一项研究，调查是否有必要实施一个新的指纹认证系统。可以找一个你们内部熟悉此项工作的人帮我们一下么？”

当本地的专家拿起电话时，弗兰克询问了一系列有关他们使用的指纹系统的问题，以及检索和储存指纹数据的能力。他们的系统是否出过故障？他们在国家犯罪信息中心（NCIC）还是仅在

本州进行指纹检索？这套系统对于每个人来说容易学习使用么？

狡猾的弗兰克悄悄地得到了其中的关键信息。答案对他来说如音乐般动听——不，他们不在NCIC检索，他们只在州犯罪信息索引（CII）中查询。

米特尼克信箱

精明的信息骗子想获悉法律执行程序方面的问题时，从不会迟疑于给联邦、州或是地方政府打电话。利用这些唾手可得的信息，社会工程师很可能会绕过企业的常规安全检查。

那就是弗兰克所需要知道的，他在这个州没有任何犯罪记录。因此，他提交了他的工作申请，并被录用。而且，一直也没有任何人出现在他的办公桌前对他说："这些先生是联邦调查局的，他们想跟你谈谈。"

据弗兰克所说，他后来成为那家公司的一名模范雇员。

放到门口

尽管我们有美丽的无纸办公神话，但在企业，每天还是继续打印出大量的纸张，而纸上打印的企业内部信息很容易泄露，即使上面印着机密并采取了安全防范措施。这里有一个故事，它将显示社会工程师如何获取你最机密的文件。

"环回"欺骗

电话公司每年都要刊印一本叫做测试号码目录的电话册。至少以前是这样，由于我还处于监督释放期（译者注：类似假释），我并不打算去问电话公司是否还在这样做。电话盗打者十分重视这本电话册，因为它包含了一个列表，上面列出了所有企业工人、技师使用的受到严密保护的号码，以及其他一些总是处于忙音的中继线测试和检查号码。在这些测试号码当中，有一个术语称做"环回"（loop-around）的号码，尤其有用。电话盗打者用它做为一个找到其它同行聊天的方法，对他们来说这无需成本。电话盗打者还把它用来做为给予对方的回电号码，比如银行。一个社会工程师会告诉银行的人，打这个电话号码到他的办公室，当银行按这个号码（环回号码）打过来时，电话盗打者就可以接到，同时还很安全，因为依据这个号码无法追踪到他。

测试号码目录提供许多极其有用的信息，从而被对信息无比渴求、内分泌激素发达的电话盗打者所利用。因此，每当新的目录发布时，都会被大量的喜欢探究电话网络的年轻人所觊觎。

米特尼克信箱

为保护企业的信息资产，企业里的每个人都需要而进行安全培训，而不仅仅是那些通过电子线路或是物理接触而访问到企业信息资产的人。

史蒂夫的诡计

无疑，电话公司不会轻易地让人得到这些目录。因此，电话盗打者必须想出创造性的办法。他们怎么做呢？一个对目录有着强烈渴望的年轻人可能会设计这样一个场景……

某日，南加利福尼亚秋天的一个傍晚，一个我称之为史蒂夫（Stevie）的人给一家小电话公司的总机室打电话，这个总机室所在的大楼负责服务区内所有家庭及企业电话线路的连接。当值班的接线员拿起电话时，史蒂夫称自己是电话公司刊印和发行打印资料部门的人。“我们刊印了你们新的测试号码目录，”他说。“但出于安全考虑，如果我们没有收到旧的目录，就不能给你们发新的。可送目录的人迟到了，如果你们把旧的目录放到门口，他经过时就能取到，并放下新的，然后继续赶路。”

毫不怀疑的接线员似乎觉得这很合理，于是照做，把目录放到大楼门口，虽然目录的封皮上用红字清楚地印着“公司机密——无用时销毁。”

史蒂夫开车过来，小心的察看四周，是否有警察或电话公司的保安人员藏在树后或在停泊的汽车里监视。没有人。他装作不经意地拾起那本令人垂涎的目录，开车走了。

这就是社会工程师轻易得到他想要的东西的另一个例子，这里就使用了那个简单的原则——“直接索取”。

谎言攻击

不只是企业的资产处于社会工程师设置骗局的危险之下，有时，企业客户也会成为受害者。做为客服人员，不可避免的会受

到挫折、讥笑和无辜的误解，有些人还会给企业的客户带来不良后果。

珍妮·爱克顿（Janie Acton）的故事

感恩节的一周，打来了一个不同寻常的电话。打电话的人说："我是客户名单部的爱德华多（Eduardo），我正与一位女士通着电话，她是执行办公室一位副总裁的秘书，她需要知道一些信息，而我的计算机坏了。我接到了人力资源部一位姑娘发来的一封写着'我爱你'的邮件，当我打开附件时，就再也不能使用我的电脑了。病毒，我中了一个愚蠢的病毒。就是这样，你能帮我查一下客户信息么？"

"当然，"珍妮回答。"它毁了你的计算机么？真糟糕。"

"是啊。"

"我该如何帮你？"珍妮问。

在这里，攻击者为了使自己听起来可信，便对想知道的信息预先做了调查。他了解到他所需的信息存储在一个叫做"客户名单信息系统"（CBIS）的系统中，并且他还知道了工作人员与系统的关系。他问："你能从CBIS中查一个账户么？"

"可以，账户号码是多少？"

"我不知道。我需要你用姓名来查。"

"好的，什么姓名？"

"希瑟·玛宁（Heather Marning）。"他拼出名字，珍妮把它输入。

"好的，我查到了。"

"很好。账户调出来了？"

"嗯哼，调出来了。"

"账户号码是什么？"他问。

"你有笔么？"

"准备好了。"

"账户号码，BAZ6573NR27Q。"

他重复了一遍号码，然后问："服务地址是什么？"

她告诉他地址。

"电话呢？"

珍妮也欣然地读给他。打电话的人向她致谢，并说再见，然后挂线。珍妮继续下一个电话，再也不去想这件事情。

亚特·锡利（Art Sealy）的调查方案

亚特·锡利放弃了为那些小出版社做自由编辑的工作，他找到了一个更能赚钱的方法，为作者和相关业务做调查。不久，他发现他的工作内容越是接近非法与合法之间的模糊界限，他就越可以收取更高的费用。从没有想到过，当然也从不知道这就是社会工程，亚特使用着与每个信息经济人都使用着的类似方法和技术，成为了一名社会工程师。他最终证明自己有此方面的天分，懂得了大多数社会工程师必须从他人身上学来的技巧。不久，他就毫无罪恶感的跨过了非法与合法之间的界限。

一个位正在写一本尼克松年代时关于政府内阁方面的书的作家打电话给我，说他想找一个能够挖掘出威廉·西蒙（William E. Simon）内幕消息的调查人。威廉·西蒙，曾任尼克松时期的财政部长。西蒙先生现已去世，但这位作家知道他的一名女下属的名字，并确切的知道她仍然住在华盛顿特区，可不知道详细地址。她的名字也未登记电话，或者至少是没有列出她的电话，这就是他之所以联系我的原因。我告诉他，好的，没问题。

这就是那种通常一两个电话就可以完成的工作，如果你知道自已是在做什么的话。通常情况下，每个地方上的公共事业公司都有可能查到这样的信息，当然，这需要些小小的谎言，但偶尔撒一个小谎无所谓吧，对么？

我喜欢使用不同的方法，只为了让事情有趣些。“我是执行办公室的某某……”这样的开场白，一直都很好用。同样还有这次使用的“我正在与某副总裁办公室的人通话”也不错。

你必须充分发挥社会工程师的潜能，把握电话另一端将与之打交道的人的配合性。这次我幸运的碰到了一位友善、热心的女士，仅打了一个电话，就得到了地址和电话，任务完成。

米特尼克信箱

绝不要以为所有的社会工程学攻击都会把骗局设计的十分复杂，以防被人轻易识破。有些攻击来去匆匆、得手即逝，更简单的攻击仅仅是，直接索取。

过程分析

珍妮肯定知道客户信息属于敏感信息，她绝不会与一位客户谈论另一位客户的账户，也不会向外部泄露客户的私人信息。但

是很自然地，当一个公司内部的人员打来电话时，情况便不同了。做为公司团队的一员，同事之间最重要的是互相帮助，以完成工作。那个客户名单部的工作人员，如果不是病毒把计算机搞坏，他自己完全可以查阅客户信息，她自然很乐意帮助一个同事。

亚特渐渐地接近了他真正想寻求的关键信息，在这一过程中他还提出了他不必知道的问题，如账户号码。然而，这个账户号码也为他提供了一个退路。万一珍妮有所警觉，他再打第二个电话时，成功的可能性便大大的增加了。因为，这个账户号码会让他给下一个工作人员打电话时，听起来更加可信。

从未有人向珍妮撒过这样的谎，打电话的人根本就不是客户名单部门的人。当然，珍妮也不应被责怪。她并不熟悉那条“在谈论客户档案信息之前，一定要知道与之谈话的人是谁”的规则，没有人告诉过她象亚特这样打来电话的危险性，公司里也没有制定这样的政策，她也从来没有培训过这方面的内容，而且她的主管也从未提及过。

预防措施

企业安全培训的一个要点就是：如果一个来访者或是打电话的人知道公司某人的名字，或是知道一些内部用语或业务程序，并不意味着他的身份不值得怀疑。而且绝对不要认为他是可信任的，从而把内部信息泄露给他，或是让他访问到你的计算机系统和内部网络。在安全培训中需要反复强调：一旦有所怀疑，必须确认、确认，再确认。

在过去，能够访问到企业内部信息是拥有权力和级别的标志。工人们往熔炉里添燃料、运转机器，员工们打字、填写报告，工头或是上司告诉他们做什么，何时做，如何做。只有工头或上司才知道一个班上的每个员工生产多少零件，工厂这个星期、下个星期、这个月底需要生产出什么颜色、什么尺寸、什么数目的产品来。

工人们负责机器、工具和原材料，老板们负责处理信息。工人只需要知道与本职工作有关的信息。

那时的情况与现在有所不同，不是么？现在，许多工厂的员工都使用某种计算机或是由计算机控制的机器。对大多数人来

说，重要的信息都直接放在使用者的桌子上，以便于他们履行自己的职责来完成工作。在现代社会，几乎每一名员工都离不开处理信息的工作。因此，企业的安全策略应遍布企业的各个地方，而无所谓职位的高低不同。每个人都应该认识到，不仅是上司或管理人员拥有攻击者想追寻的信息。今天，每个层次级别上的职员，甚至是不使用计算机的人，都有可能成为攻击者的目标。而公司新近雇用的客服人员则是社会工程师最容易突破的薄弱环节，企业的安全培训和安全策略务必要加强这方面的注意。

## 第四章建立信任

这些故事可能会导致你认为我把业务中接触到的每一个人都看成十足的傻瓜，都很乐意地、甚至是渴望着把他或她所拥有的每一个秘密泄露出去。社会工程师知道，这是不可能的。为什么社会工程的攻击容易得手呢？这不是因为人们的愚蠢或是缺乏常识，而是因为，我们人类很容易被操纵而把信任用错了地方，因此被欺骗。社会工程师早已料到会受到阻力和怀疑，他随时准备着把人们对他的怀疑扭转。一个优秀的社会工程师策划攻击时如同下象棋，预先想到对方可能会提出什么样的问题，从而把合适的答案准备好。他的一个很常用的技巧就是给受骗者建立信任感，一个骗子如何才能获得你的信任呢？相信我，他能够。

### 信任：欺骗的关键

社会工程师越把情况营造得像普通的业务联系，就越能减少怀疑。当人们没有疑心时，得到他们的信任就很容易了。一旦取得你的信任，如同吊桥放下，城门打开，他就可以入内随心所欲地取得他所需的信息。

注：你也许注意到我在提及社会工程师、电话盗打者和设计骗局的人时，大多数情况下用的是“他”。这不是偏见，这只是反应了一个事实——从事这些领域的人大都是男性。但尽管女社会工程师很少，可这个数字正在增长。不要仅仅因为听到了一位女性的声音而放松了你的警觉，女社会工程师还是有的。事实上，女社会工程师有着独特的优势，利用她们的女性特征来得到对方的配合。本书以后的内容中将会出现少量的女性社会工程师。

### 第一个电话：安德瑞亚·洛佩兹（Andrea Lopez）

安德瑞亚·洛佩兹在她工作的音像店接到了一个电话，她立刻微笑起来（当一位客户特意打来电话对服务表示满意时，总会让人高兴）。打电话的人说，在他们店里得到了非常好的服务，他想给写封信告诉他们的经理。他询问经理的名字和通信地址，她告诉他名字是汤米·艾里森（Tommy　Allison），并把通信地址也给了他。就在要挂电话时，他又有了一个想法，他说：“我还想写给你们公司总部，那儿的电话是多少？”她也告诉了他。他道了谢谢，并说了些她的服务十分让人满意之类的话，然后再见了。“像这样的电话，”她想，“总能让上班的时间过的快些，如果多有些这样的人就好了。”

第二个电话：吉妮

“欢迎致电音像工作室，我是吉妮，需要帮忙么？”

“嗨，吉妮，”打电话者热情的打招呼，听起来就像每个星期都给吉妮通话似的。“我是汤米·艾里森”，863店森林公园的经理。我这儿有一位客户，想租《洛奇5》，可我们这儿已经没有拷贝了，你能查一下你们那儿有么？”

过了一会儿，她回答：“是的，我们还有三个拷贝。”

“好的，我问一下客户是否愿意过去，谢谢你。如果有任何需要，请致电汤米，我很乐意为你效劳。”

接下来的几个星期，吉妮又接到过三、四次汤米寻求帮助的电话，这些要求似乎都很正常，他总是十分友善，没有故意接近她的意思。同时，稍稍有些唠叨。如“你听说橡树园的大火了么？一连串的街道都封掉了，”类似的话。对于日常工作来说，这些电话可以让人得到片刻的休息，吉妮总是乐意接到他的电话。

一天，汤米打来电话，听上去有些焦虑，他说：“你们的计算机出过问题么？”

“没有，”吉妮回答。“怎么了？”

“有个人开车把电线杆撞了，电话公司的修理人员说城市的一部分地区没办法打电话和上网，直到他们修好。”

“哦，不会吧。那个人受伤了么？”

“他们把他送到救护车上了。别管这些了，我需要你帮个忙。我这儿有一个你们的客户，想租《教父2》，但他没带租片卡，你能帮我确认一下他的信息吗？”

“是的，当然。”

汤米说出客户的名字和地址，吉妮在计算机中找到，然后告诉汤米客户的账号。

“有过期未还和欠款记录么？”汤米问。

“没有。”

“好的，很好。我手工给他登记一下账户，计算机故障恢复之后再录入数据库。而且，客户还想用在你们店使用的维萨卡（Visa）付账，但他也没带。他的卡号和有效期是多少？”

吉妮都告诉了他。汤米最后说：“嗨，谢谢帮忙，回聊！”

道伊尔·罗尼甘（Doyle Lonnegan）的故事

罗尼甘可不是一个普通的年轻人，他过去是一个收藏家，欠

了不少赌债，如果不是这些赌债弄得他焦头烂额的话，他还会偶尔继续他的爱好。在这个故事里，他仅仅往一家音像店打了几个电话，就得了一笔现金。这听起相当不错，因为他的“客户”没有人知道如何设计这个骗局，他们需要像罗尼甘这类人的知识和才能。

每个人都知道，当他们在牌桌上运气差或是犯错误而输钱时，是不会用支票来代替赌资的。可为什么我的这些朋友们还要跟一个没带钞票的骗子赌钱呢？不要问了，也许他们的智商有点儿问题，但他们是我的朋友，我又能怎么办？

这个家伙没带钱，于是他们收了他的支票。让你说，他们应该开车把他带到自动柜员机那儿去吧？本应这样做的。但他们没有，他们收了一张支票，3230美元。不用想，这是张空头支票。还有什么其它可能呢？于是，他们给我打电话，问我能帮忙么？我不再用门去挤别人的手指了（译者注：指暴力手段），而且，现在有更好的办法。我告诉他们，我要30%的佣金，看我的本事吧。他们给了我他的名字和地址，我用计算机找到离他最近的音像店。我并不着急，先后打了四个电话来讨好音像店的经理，然后，我就得到了那个骗子的维萨卡号。我有一个朋友开了一间半裸吧（译者注：裸露半身的脱衣舞酒吧），用了50美元，把那个骗子所欠的赌资当做酒吧消费从他的维萨卡上划出，让他给老婆解释去吧。你认为他会找信息卡公司说他没有花这笔钱吗？好好想想。他知道我们知道他是谁，而且如果我们可以拿到他的维萨卡号，他会认为我们还可以做更多的事情，因此，这件事没什么可担心的。

过程分析

汤米打给吉妮的第一个电话仅仅是为了建立信任，当真正的攻击开始时，她已经放松了警惕并认同汤米所声称的身份——另一家连锁店的经理。有什么理由不接受他呢？她已经认识了他。当然，仅仅是通过电话联系，可他们已经建立了工作上的友谊，那是信任的基础。一旦她认为他是可以相信的人——同一家公司的一位经理，信任感就已经建立，剩下的事就顺其自然了。

米特尼克信箱

建立信任的欺骗技术是社会工程学最有效的策略之一，你务必要考虑你是否真正认识与你谈话的人。在一些不常见的情形

下，对方很可能不是他自己声称的那个人。因此，我们必须学会观察、思考和提问。

主题变奏：攫取信用卡

建立信任感，不一定非得给受骗者打上一系列的电话，如上文中讲述的案例。我想起一个亲身经历的故事，它建立信任感只用了5分钟。

惊奇吧，爸爸

有一次，我与汉瑞（Henry）和他父亲坐在一家餐馆。谈话中，汉瑞责怪他父亲把信用卡号像电话号码一样随便泄露给别人。

“当然，买东西时必须使用信用卡号，”汉瑞说。“但是把你的卡号告诉一家商店，并让他们记录下来，那是非常不明智的。”

“我只在音像工作室这么做过，”康克林（Conklin）先生说，“但我每个月都会查看我的维萨卡记录，如果他们多收费用，我会知道的。”

“当然，”汉瑞说。“但他们一旦知道了你的卡号，别人就很容易弄到了。”

“你是指不怀好意的店员么？”

“不，我是指任何人，不仅仅是店员。”

“你在信口开河，”康克林先生说。

“我可以现在就打电话，让他们告诉我你的维萨卡号，”汉瑞立刻大声回应道。

“不，这不可能，”他父亲说。

“我可以在五分钟之内搞定这件事，就在你的面前，连桌子我都不会离开。”

康克林先生看起来有些紧张，他自己感觉到了这种紧张，但并不想让别人知道。“你根本就不知道你在说什么，”他急促地说，并掏出钱包拿出50美元甩到桌子上，“如果你能做到你说的话，这是你的了。”

“我不想要你的钱，爸爸。”汉瑞拿出手机，询问他父亲是哪一个音像店分店，然后打电话给查号台找到分店的电话号码以及谢尔曼橡树园（Sherman Oaks）分店的电话号码。接着，他打电话给谢尔曼·奥克分店，几乎用了跟上一个故事完全一样的方法，很快得到了经理的名字和分店的店号（译者注：如上文中提到的863分店）。然后，他打电话给登记着他父亲账户的分店，利用刚

刚得到的名字和分店店号来假扮分店经理。接着使用相同的手法："你们的计算机没出问题吧？我们这儿的计算机时好时坏。"听到了她的回答后他接着说，"嗯，是这样，我这儿有一位你们的客户想租一部片子，可我们的计算机现在坏掉了，我需要你帮忙查一下客户的账号以确定他就是你们店的客户。"

汉瑞给出他父亲的名字，使用了一个稍有不同的方法，他请求对方把账户信息读出来：地址、电话，开户日期，然后说："嗨，是这样，我这儿有一大堆等着的客户，他的信用卡和有效期是多少？"汉瑞一支手在耳边拿着手机，另一支手在餐巾纸上写。打完电话，他把餐巾纸推到瞪着眼睛、张着嘴巴的父亲面前，可怜的父亲看上去完全震惊了，似乎他的信任系统已被完全颠覆。

过程分析

当某个不认识的人询问你某事时，想想自己是什么态度。如果一个衣衫褴褛的陌生人来到你门前，很可能你不会让他进去。如果是一位衣着得体、皮鞋明亮、发型完美，举止优雅并面带微笑的陌生人，你可能就会放松警觉。也许他就是现实生活中的占森（译者注：电影《十三号星期五》中的杀人狂）呢？但你仍然愿意相信他，只要他看起来正当，手里也没有握着餐刀。

米特尼克信箱

人们习惯的认为自己在任何特定的事务中不大可能走进骗局，否则至少也得有理由相信这是个骗局。大多数情况下，我们权衡风险，然后假定别人没有恶意。这就是有教养人的一般行为，至少那些没有被操纵、利用或被骗过一大笔钱的有教养的人这样认为。在儿时，我们的父母告诫我们不要相信陌生人，也许在当今的工作环境下，我们所有的人都就应谨记这个陈旧的规则。

工作中，人们总是会有各种各样的请求。你有这个人的电子邮件地址么？最新的客户名单在哪儿？谁是这个项目本部分的分包商？请发给我最新的计划更新。我需要新版本的源代码。有时，做出这些请求的人你并不直接认识，或是公司其他部门的人，或是他们自己说是其他部门的人。但如果他们提供的信息是正确的，并且看来熟悉公司内情（"玛丽安说……"、"这里是K16服务器"、"……新产计划第26次修订版"），我们便把信任圈扩大他们身上，轻率的满足了他们的请求。

当然，我们也许会有些困惑的问自己："为什么这个达拉斯（Dallas）分厂的人想知道新的产品计划？"或是"说出服务器的名称会有害处么？"等等这类问题，如果答案看上去合情合理，对方的言行也比较可靠，我们便会放松警惕，恢复相信同事的习惯，并满足（有理由的）对方的请求。

绝不要认为攻击者只会把目标锁定到使用计算机的人身上，收发室的人也可能是目标。"能帮个忙么？把这个放到公司内部的邮袋。"收发室的人可不知道它是一张带有特殊程序的针对首席执行官秘书的软盘。这样，攻击者本人就拥有了首席执行官的邮件拷贝。不会吧？这事情真得会在企业中发生么？答案是，绝对可能。

一美分的手机

许多人都在寻找好的机会，不达目的不罢休。社会工程师不然，他们找到办法使机会变得更好。比如，某公司进行一项诱人的市场优惠活动，社会工程师就会想办法扩大他的利益。

不久以前，一家全国性的无线通讯公司发起了一个大规模的促销活动，只要你登记接受一种资费方式，便可以得到一部全新的手机，只收一美分。对于一个精明的消费者来说，在登记一种资费方式之前，有好多问题要问清楚。通讯服务是模拟还是数字的，或是两者结合？每个月的免费通话时间是多少？是否包含漫游费……等等，等等，尤其重要的是资费合同时限——你承诺的资费方式是多长时间，几个月还是几年？

想像一个这样的情景，一位费城（Philadelphia）的社会工程师被通讯公司提供的一款十分便宜的手机所打动，但他讨厌与其捆绑的资费方式。没什么大不了的，他也许使用下面的方法来解决此事……

第一个电话：泰德（Ted）

他首先打给位于西吉拉德（West Girard）的一家电器连锁店。

"电子商城，我是泰德。"
"嗨，泰德，我叫亚当。是这样，我在前几天晚上，跟你们的

一个男销售员谈到一个手机，我说一旦决定了就给他打电话。可我忘了他的名字，你们值夜班的人是谁？”

“不只一位，是威廉么？”

“不知道，也许是吧。他长什么样？”

“高个子，瘦瘦的。”

“我想是他吧，他姓什么来着？”

“哈德利。哈 - 德 - 利（H--A--D--L--E-- Y.）”

“是的，是他。他什么时候上班？”

“我不知道他这星期的排班，但上夜班的人5点到。”

“好的，那我试试晚上找他。谢谢，泰德。”

第二个电话：凯蒂（Katie）

第二个电话打给位于北广街（North Broad Street）的连锁店。

“嗨，电器商城。我是凯蒂，需要帮忙么？”

“凯蒂，嗨！我是威廉·哈德利，西吉拉德店的。今天过得怎么样？”

“有点儿忙，什么事？”

“我有一位顾客想购买那个一美分的手机，你知道这个手机的资费捆绑吧？”

“是的，上星期我售出了一些。”

“你那儿还有这种资费捆绑的手机么？”

“还有一堆呢。”

“很好。我刚售出了一个这种手机的资费，顾客通过了信用记录（译者注：美国通讯公司会查询手机用户过去的使用记录，以确定用户是否具备享受某一资费方式的资格），我们也签了资费合同。我查了一下该死的存货记录，却没有这种手机了。这让我很难做，你能帮个忙么？我让他到你们店去买一美分的手机，你卖给他后开张发票。他买到手机后会给我打电话，然后我再告诉他怎么用。”

“好的，当然可以。让他来吧。”

“太好了，他叫泰德，泰德·岩西（Ted Yancy）。”

一个自称泰德·岩西的人来到北广街连锁店，凯蒂开了一张发票，把一美分的手机卖给他，完全依照她的“同事”交待给她的事情，从而彻底地掉入骗局。付钱时，这个顾客的钱包里一枚硬币也没有，于是他到收款台的零钱碟中拿了一枚，交给她完成登记。他甚至一分钱都没有花就得到了那部手机。

过程分析

人们会很自然地相信熟悉公司内部的业务流程和专业用语，并声称自己是公司同事的人。这个故事中的社会工程师就是利用了这一点，通过了解促销活动的细节，扮做公司的职员，并要求另一个分店人员的帮助。这种事情在各零售店之间以及一个公司的各部门之间经常发生，这是因为人们没有机会接触，天天与从未见过面的同事打交道。

入侵FBI

人们通常不住地去想他们的公司会在网站上提供什么资料。我在洛杉矶一个电台做每周一次的脱口秀节目，节目制作者在网上做了一次搜索，发现了一份访问国家犯罪信息中心（NCIC）的操作说明拷贝。不久他发现，真正的NCIC操作说明原件就在网上，这是一份相当敏感的文档，它记录着从FBI的国家犯罪记录数据库中提取信息的所有操作说明。对于执法部门，这份说明就是一本从国家数据库中提取犯罪记录和罪犯信息的格式和代码的操作手册。国家的所有执法部门都可以依据他们所属的权限从同一个数据库中查询有助于办案的信息，手册里包含了数据库中用来标明各种信息的代码，从各种各样的纹身到各式各样的轮船外壳，再到失窃纸币和债券的面额。

任何人接触到这本手册的人都可以在上面找出从国家数据库中查找信息的命令和语法规则，然后依据手册上的步骤指导，再加一点胆量，人人都可以从数据库中提取信息，而且手册还提供使用数据库系统的服务支持电话。也许你的公司也有这样的包含着产品代码或是查询敏感信息的代码手册。

FBI几乎肯定不知道如此敏感的资料暴露在网上，我想如果他们知道此事一定会很恼火的。一份拷贝是由俄勒冈州政府部门放到网上的，另一份是由得克萨斯州的执法机构传到网上。为什么？这都是因为，也许某人觉得这些信息可能没什么价值，放到网上也不会有什么害处。也许有人为了内部人员使用上的方便，而它放到内网上，却从未想到会被在网上使用搜索引擎（如Google）的人找到，包括仅仅是好奇的人、还有想当警察的人、黑客，以及有组织的犯罪团伙。

接入系统

利用这样的信息来欺骗有政府或企业背景的人，使用的准则是相同的：由于社会工程师知道如何访问特定的数据库或应用程序，或是知道公司的服务器名称等类似的事情，他因此具备可信性，这种可信导致信任。一旦社会工程师拥有了这样的代码，获得所需信息就十分简单。在这个例子中，他首先给当地的州警察局电讯室打电话，针对手册上的一个代码，提出问题。比如，犯罪代码。他可能这样说，“我在NCIC做犯罪记录查询时，碰到‘系统发生问题’的错误提示。你做记录查询时碰到过这种情况么？能帮我试一下么？”或者他会说正在查询WPF（警方用语，被通缉人的档案）。电话另一端，电讯室的工作人员就会意识到对方熟悉查询NCIC数据库的操作程序和命令，除了受过训练的人，谁会知道这些操作程序呢？

工作人员确定她的系统运行正常后，谈话可能像这样进行：

“我可以帮点儿忙。你要查什么？”
“我要查瑞尔顿·马丁的犯罪记录，出生日期66年10月18日。”
“索什（SOSH，执行部门的人有时把社会保险号简称为索什）是多少？”
“700-14-7435。”
找到名单后，她可能这样说：“他的犯罪记录代码是2602。”

现在，攻击者只需到NCIC的网站上查一下这个号码的含义了——这个人有一桩诈骗的犯罪记录。

过程分析

一个出色的社会工程师一刻也不会停止思考闯入NCIC数据库的办法，往当地警察局打上一个电话，花言巧语一番让对方认为自己是内部人员，这就足以能够得到他所需的信息。下一次，他只需使用相同的借口往另一个警察局打电话就是了。

你也许会吃惊，往警察局或是州政府打电话不危险吗？那攻击者不是冒了很大的风险？

答案是不……因为一个特殊的理由。执法人员像军人一样，从他们第一天到学院开始等级制度观念就已经根深蒂固了。只要社会工程师伪装成一个警官或助理官员——比和他谈话的人等级更高——受骗者将被精心学习的课程支配，不要怀疑比你职位更高的人。等级，换句话说就是拥有特权，特权不会被等级低的人挑战。

但是不要认为执法部门和军事部门是社会工程师唯一可以利用等级制度的地方，社会工程师经常在商业攻击中像使用武器一样利用公司的职权或等级——就像这一章的许多故事所示范的那样。

预防措施

保护你的消费者

在这个电子时代许多公司出售商品给消费者时将信用卡信息存档。理由是：解决了消费者每次进入商店或Web站点购物时都要输入信用卡信息的麻烦。然而，这种做法应该避免。

如果你必须将信用卡号存档，使用复杂的编码或者存取控制来进行安全防范必不可少。员工需要培训识别像这一章中社会工程师的一些诡计。那些从没亲眼见过但在电话里成为朋友的同事可能并不像他或她声称的那样。他也许并不“需要知道”客户的敏感信息，因为他可能根本就不在这家公司工作。

米特尼克信箱

每个人都应该知道社会工程师的一贯手法：尽可能地搜集一些关于目标的信息，利用这些信息增加内部人员的信任。然后直取要害！

聪明的信任

不只是有明显的敏感信息的人——软件工程师，研究与开发（R&D）人员，等等——需要防范入侵者攻击。你的公司的几乎所有人都需要训练保护企业防范商业间谍和信息窃贼。

一切的基础应该从一个企业信息资产调查开始，分离地看待每一个敏感的，关键的或贵重的资产，并寻找攻击者使用社会工程学策略可能危及这些资料安全的方法。对有权访问这些信息的人进行的适当培训应该有计划地围绕这些问题的答案。

当一个你不认识的人请求获得一些信息或材料，或要求你在你的电脑上完成任何操作时，让你的员工问他们自己一些问题。如果我把这些信息给了我最坏的敌人，它会被用来伤害我或我的公司吗？我十分了解被要求输入到我的电脑的这些命令的潜在影响吗？

我们不想抱着对我们遇到的每一个陌生人的怀疑度过一生。但是我们的信任越多，下一个看上去十分友好的社会工程师就会来到我们的城市里，欺骗我们，获得我们公司的所有信息。

什么属于你的Intranet（企业内部互联网）？

你的Intranet的一部分可能开放到了外部世界中，而另一部分则限制只有员工能使用。你的公司有没有仔细地确认受保护的敏

感信息没有被放到访客易接近的地方？当上次公司的一个人在Intranet上查看到任何敏感信息并不经意地提交到了Web站点的公共访问空间的时候？

如果你的公司执行代理服务保护企业应对信息安全威胁，这些服务在最近的检查中确认被适当的配置了吗？

事实上，有人检查过他们的Intranet安全性吗？

## 第五章我来帮你

当我们遇到头痛的事情时，如果有个经验丰富、技术高超的人来帮忙，我们一定会很感激。社会工程师了解这一点，并懂得如何利用它。他还知道如何制造一个麻烦，然后帮你解决以获得你的感激，最后利用你的感激之情来获取信息或得到你的一些小关照，这将把你的公司或是你个人置于不利的地步，而你可能永远不知道你已经遭受损失。下面是一些社会 工程师“帮忙”的典型方法。

### 网络故障

日期/时间：2月12日星期一，15:25
地点：斯达伯德（Starboard）造船厂办公室

第一个电话：汤姆·狄雷（Tom Delay）

“簿记处，汤姆·狄雷。”
“嗨，汤姆，我是服务中心的艾迪·马丁（Eddie Martin）。我们正在检修计算机网络，你们部门有人在线时遇到问题了么？”
“嗯，据我所知没有人。”
“你这儿也没什么麻烦吧？”
“没有，还算正常。”
“好的，很好。是这样，我们正在给可能发生网络问题的人打电话，如果你的网络连接中断请立即告诉我们，这很重要。”
“听起来可不妙，你觉得它可能出问题么？”
“我们希望不会，但一旦有情况，请打电话好么？”
“这你放心。”
“是这样，如果你们的网络连接掉线，很可能是你这儿的问题……”
“那可没准儿。”
“所以我们会检修你这里的网络，我把我的手机号留给你，如果有需要你可以直接找到我。”
“太好了，请说。”
“555 867 5309。”
“555 867 5309，好了，谢谢。你叫什么来着？”
“艾迪。听着，还有一件事。我需要检测一下你的计算机连接端口，看一下你的计算机哪里贴着一个大概写着“端口号”字样的标签？”
“稍等，没有，我看不到有这样的东西。”

“好吧，这样，你再看计算机的后面，能找到网线么？”
“是的。”
“顺着线找到它的插头，看看它的插口上是否有一个标签。”
“稍等一下，再等等，我必须蹲下离近些才能看清楚。好的，上面写着6杠47（6-47）。”
“很好，那就是我们记录的端口号，只是为了确认一下。”

第二个电话：技术支持

两天后，一个电话打到该厂的网络管理中心。

“嗨，我是鲍勃（Bob），我现在簿记处汤姆·狄雷的办公室。我们正在检修网线故障，请你封掉6-47的端口。”

技术支持人员回答说很快就封掉，并说可以恢复的时候再通知他们。

第三个电话：敌人的帮助

一个小时后，一位自称艾迪·马丁的人在Circuit City购物时，他的手机响了。他发现是造船厂的号码，便迅速地转到一个安静的角落接听手机。

“服务中心，艾迪。”
“哦，嗨，艾迪。有事找你，你在哪儿？”
“我么，嗯，我在机房，你是？”
“我是汤姆·狄雷。伙计，很高兴能找到你。或许你还记得前两天给我打过电话吧？我的网络连接可能像你说的那样断掉了，我有点不知道怎么办。”
“是的，刚刚好几个人都说掉线了，我们在今天晚上会处理此事，好么？”
“不！见鬼！如果断线那么长时间，就要耽误事了。能尽量帮帮我么？”
“事情很紧？”
“我有事得赶紧弄，有没有可能在半个小时之内处理好？”
“半个小时？你也太着急了。嗯，这样，我放下手里的活，看看能不能帮你解决。”
“嗨，艾迪，真是谢谢你了。”

第四个电话：搞定

45分钟后……

“汤姆？我是艾迪，去看看你的网络连接。”

不一会儿：

“噢，好了，它好了，太棒了！”

“很好，很高兴为你解决了。”

“是啊，十分感谢！”

“听着，如果你不想让它再出毛病，要安装一个软件，几分钟就可以了。”

“可现在不太合适。”

“我理解，但如果下次网络连接再出毛病，这会让我们都省心的。”

“好吧，如果只需几分钟的话。”

“你照这样做……”

艾迪指导汤姆从一个网站下载一个小程序，下完之后，艾迪叫汤姆双击它。汤姆照做，但反馈说：“不行，什么反应都没有。”

“噢，真讨厌。程序一定有什么地方出错了，算了吧，我们可以下次再试。”接着他指导汤姆删除掉程序，以使其不能恢复。

整个过程花费时间，十二分钟。

攻击者的故事

每当鲍比·华莱士（Bobby Wallace）接到这样的一项任务时总觉得很可笑，他的客户总是在为什么需要这种信息的问题上闪烁其词。这件案例中，他只想到两个原因：也许他们代表某个意图收购斯达伯德造船厂的组织，因而想知道造船厂真正的财务现状，尤其是被收购方想对潜在购买者刻意隐瞒的东西。或者，他们代表投资方，认为他们的资金在使用上有些可疑，并想知道是否有些管理人员私自开设了小金库。

也许他的客户并不想让他知道真正的原因，因为如果鲍比知道了那些信息的价值，他可能会索要更多的酬金。

有许多破解企业最机密文档的方法，鲍比在制定计划前花了几天时间做选择并进行了小小的测试。他决定使用一个称为“接近”的他尤其喜欢的方法，让对方自己落入圈套，他会自动请求攻

击者的帮助。

首先，鲍比花39.95美元在便利店买了一部手机，然后打电话给那个他选做目标的人，冒充公司服务中心的人哄骗对方在网络连接出问题时给他打电话。为了使事情看上去不那么明显，他故意等了两天才给网络管理中心（NOC）打电话。他声称在为汤姆（他的目标）检修网络问题，并要求NOC把网络连接禁止掉，鲍比知道这是整个计划中最棘手的部分。在许多企业，服务中心与NOC有着紧密的工作关系，实际上他知道服务中心通常就是IT部门的一个分部。但NOC接电话的人懒得问那个解决网络问题的服务中心人的名字，并同意禁止掉对方要求的网络端口。这一切搞定之后，汤姆就被完全的从企业内网上隔离了，不能从服务器上检索文件，也不能与同事交换文件、下载邮件，或甚至不能把数据传到打印机。在当今的世界，这如同居住在一个洞穴中。

正如鲍比所预想的，他的手机很快就响了。当然，他尽量使自己听上去十分愿意帮助这个不幸的同事，然后给NOC接电话把网络连接恢复。最后，他打给汤姆再次控制了他，这一次由于帮他解决了问题，令对方心存感激，于是汤姆同意下载一个软件到他的计算机上。当然，他同意下载的软件并不是鲍比所说的那样，是为了防止网络连接的再次中断，它实际上是一个特洛伊木马，一个用来对付汤姆的计算机的应用程序（特洛伊是一种原始的把敌人带到对方内部的欺骗方法）。汤姆回复说双击程序后没有任何反应，这是故意让他看不到发生任何事情的，实际上这个小巧的应用程序正在安装一个允许渗透者悄悄访问汤姆计算机的秘密软件。利用这个软件，鲍比可以完全的控制汤姆的计算机，这称为远程命令行解释器。当鲍比访问汤姆的计算机时，他可以查找他感兴趣的财务文件并拷贝下来，然后，在方便时检查它们是否包含他的客户寻求的信息。

专业术语

特洛伊木马：一种包含恶意或会造成危害的代码，用来损坏受害者的计算机或文件，或是从受害者的计算机和网络上获取信息。某些特洛伊木马会隐藏在操作系统中暗中监视击键或操作，或者通过网络连接来执行一些入侵命令，而这一切是在受害者意识不到的情况下进行的。这还不是全部，入侵者还可以在任何时候回到这台计算机上搜索电子邮件和私人备忘录，并对可能揭示出敏感信息的词进行文本查找。

在哄骗目标安装了特洛伊木马程序的当晚，鲍比就把手机扔到了垃圾桶里。当然，在扔之前他首先小心的删除了通话记录并拔出了电池。这是他最后要做的事情，让人再也拨不通这个电话号码。

过程分析

攻击者设计一个圈套来使对方认为自己的计算机存在问题，实际上，根本没有。或者，问题还未发生，但攻击者知道它会的，因为他将使之发生，然后他再假扮解决问题的人。这次攻击中的程序安装对于攻击者来说更是奖赏，他事先埋下了伏笔，当目标发现问题时，会自动打电话恳求帮助。攻击者只需坐在那儿等电话响就是了，可以把这次攻击看做是一次反向的社会工程学——攻击者迅速获得了信任，从而使目标主动打电话给他。如果你打电话给某个你认为是服务中心的人，你会要求对方证明自己的身份吗？这就是攻击者想制造的效果。

专业术语

远程命令行解释器：接受文本命令来执行某种功能或运行程序的非图形操作界面。通过利用漏洞或在目标计算机上安装木马，攻击者可以获得对命令行解释器的远程访问权。

反向社会工程学：攻击者设计的一种情形，受骗者碰到问题时会联系攻击者求助。另一种反向社会工程学是对付攻击者的，被攻击目标发现了对方是攻击者后，利用心理影响尽可能的从攻击者身上套出信息以保护企业的信息资产。

米特尼克信箱

如果某个陌生人帮了你的忙，然后要你帮他，不要不经过慎重考虑就回报他的帮助，要看对方要你做的是什么。在类似上面的这个骗局中，社会工程师找了一个计算机知识很少的人。他知道的越多，就越可能产生怀疑，或越能断定是被骗了。计算机白痴——对计算机操作和知识了解很少的人，则很容易遵从你的指示。他太容易掉入“只需下一个小程序”这样的陷井了，因为他对一个软件程序可能造成的损害一无所知。而且，他很可能不知道他冒着风险放到网络上的信息的价值。

给新来的女孩帮个小忙

攻击者喜欢把目标锁定在新来的雇员身上，他们认识的人很少，也不了解工作程序，什么该做，什么不该做。而且，一旦给其留下良好的第一印象，他们便会殷切地显示出对你的配合和快速地回应。

安德鲁的帮助

“人力资源部，安德鲁卡尔霍恩（Andrea Calhoun）。”

“安德鲁，嗨，我是亚力克斯（Alex），企业安全顾问。”

“什么事？”

“今天好么？”

“还好。需要帮忙吗？”

“是这样，我们正在策划一个新员工的安全培训，需要集结一些人测试一下，我想要上个月所有新进员工的名单和电话号码。你能提供给我么？”

“要到今天下午我才能给你，可以么？你的分机是多少？”

“当然，可以。我的分机是52……，噢，嗯，我今天大部分时间要开会，我回到办公室后打给你吧，大约4点左右。”

亚力克斯4点30分打来电话，安德鲁已经把名单准备好，然后在电话中读出了名字和分机号。

罗丝玛丽的消息

罗丝玛丽摩根（Rosemary　Morgan）很满意她的新工作，以前她从未在杂志社做过，她发现这里的人比她想像中友善的多（大多数杂志社职员都是在没完没了的压力下，在每一次发行最后期限前出版杂志的），而星期二早晨的一个电话再次确认了她的这种印象。

“是罗丝玛丽摩根吗？”

“是的。”

“嗨，罗丝玛丽，我是比尔乔迪（Bill　Jorday），信息安全部的。”

“有事吗？”

“我们部有人跟你谈过最佳安全操作规程么？”

“我想没有。”

“那好，我们开始。首先，我们不允许任何人安装从公司外部带来的软件，因为我们不想承担使用未经授权软件的责任。而

且，也为了避免这些软件可能携带蠕虫或病毒的风险。”

“好的。”

“你了解我们的电子邮箱规则么？”

“不。”

“你现在的电子邮箱是什么？”

“Rosemary@ttrzine.net”

“你是用Rosemary做用户名登录的么？”

“不是，我用的是R_Morgan。”

“好的。我们想让所有的新员工都意识到，打开任何一个未知邮件的附件都是危险的。蠕虫、病毒四处泛滥，并通过你似乎认识的人的邮件发来。所以，如果你收到一封意料之外的带有附件的邮件，一定要向发信方确认此信真得是由其发出。你懂了么？”

“是的，这我已经知道了。”

“很好。我们的规定是每90天换一次密码。你上一次改变密码是什么时候？”

“我才来了三个星期，还用着一开始设置的密码。”

“好，很好，你可以等到90天后再换。但我们需要确定大家不使用很容易猜出的密码，你使用的密码是由字母和数字组成的么？”

“不是。”

“我们要确定一下，你现在用的密码是什么？”

“我女儿的名字——Annette（安妮特）。”

“那可真不是一个安全的密码，你不应该在密码里包含家庭信息。嗯，我看看……，你可以和我一样，使用你现在的密码做为新密码的开头，每当更换时加一个当前月份的数字。”

“那如果我现在换的话，现在是三月，就应该是three或是-three？”

“那随你便，你更愿意用哪一个？”

“我想用Annette-three.”

“好的。你想让我为你演示一下如何改密码的么？”

“不用，我知道。”

“好。还有一件事得说一下，你的计算机上装有防病毒软件，保持更新非常重要。千万不要禁止自动更新功能，即便在它每次运行时速度会变慢。好么？”

“好的。”

“很好。你有我们的电话号码么？如果计算机出问题可以打给我们。”

她没有。他告诉她号码，她认真的记了下来，然后继续工作，并再一次地为受到热心的关怀感到欣慰。

过程分析

这个故事继续加强了此书的基本主题，你也将看到在整本书中都包含着这一主题：尽管社会工程师的最终目标不是从对方身上获取最普通的信息，但这些信息却是其目标的信任书。利用企业关健岗位上的员工那里得来的某个账号和密码，攻击者可以成功打入内部并找到任何他想找的信息。有了这些信息，如同找到开门的钥匙，把它们握在手中，他可以自由地出入企业的各个地方并找到他寻觅的宝藏。

米特尼克信箱

在企业的新员工可以访问任何计算机系统之前，必须进行培训以遵从良好的安全操作规程，尤其是有关绝不要泄露口令的规则。

不象你认为的那样安全

“在保护敏感信息上所做欠妥的企业仅仅是因为粗心大意。”许多人都会同意这个说法。而生活如果简单易懂的话，这个世界就会更好。事实却是即便企业付出相当的努力来保护机密信息，可还是存在着严重的风险。下面的故事再一次举例证明，认为由经验丰富、胜任的职业安全人员布置的安全操作规程牢不可破的想法，只是在愚弄自己。

斯蒂夫克莱默（Steve Cramer）的故事

这片草地不大，没有播撒昂贵的草种，也没人羡慕。当然，也就没有足够的理由买一台坐式割草机了，那一定很好使，毕竟他一次也没用过。斯蒂夫很乐意用手工割草机割草，因为花的时间会更长些，而这种家务事还给他提供了一个便利，使自己专注于自己的想法，而不是听安娜（Anna）讲述她工作的银行里那些人的故事或是解释为他所做的各种事情，他讨厌“夫妻表”（译者注：夫妻间为增进感情而做的一些小事，如聊天、下厨等）上的内容成为他周末的全部。当12岁的皮特绝顶聪明地加入游泳队的时候，他的心里一下子亮堂起来。现在，他每个星期六都要在训练场或是去接他，不用再陷入没完没了的家务事上了。

有些人可能认为斯蒂夫在双星医疗产品厂（GeminiMed Medical Product）的工作十分无聊，斯蒂夫却认为他在挽救生

命，他知道自己从事的是具有创造性的工作。画家、音乐家、工程师，在斯蒂夫看来都有着与他相同的挑战性——他们都创造别人从未做过的东西。他最近所做的，是一件新型的智能心脏支架，迄今为止，可能是他最值得骄傲的成就。

在这个不寻常的周六，斯蒂夫十分苦恼，都快11点半了，草地也几乎清理完，但是在思考如何降低心脏支架的动力消耗方面却没有丝毫的进展。这是他最后的障碍，虽然锄草时最适合思考这样的问题，但他一点办法也没想出来。

安娜来到门口，头上围着打扫卫生时总戴着的佩斯利（paisley）牛仔头巾。“电话，”她冲着他喊。“你公司的电话。”

“是谁？”斯蒂夫回喊道。

“叫什么拉尔夫（Ralph）的，好像。”

拉尔夫？斯蒂夫想不起医疗厂有叫拉尔夫的人会在周末打电话给他，也许安娜把名字听错了吧。

“斯蒂夫，我是技术支持部的雷蒙派瑞兹（Ramon Perez）。”

雷蒙？天知道安娜怎么会听成一个西班牙人的名字拉尔夫？斯蒂夫很奇怪。

“这是一个善意的来电，”雷蒙接着说。“有三台服务器当掉了，我们认为可能是蠕虫，必须清除驱动器，然后恢复备份文件。我们应该能够在星期三或星期四令你的文件正常使用，如果幸运的话。”

“这真让人无法接受，”斯蒂夫尽量平静的说，努力压制住自己的沮丧。这些人怎么如此愚蠢？他们真的认为他没有这些文件也可以在整个周末和下个星期的多半个星期工作么？“不行，我要用家里的电脑连线，只需两个小时，我要访问我的文件。你听明白我的意思了吗？”

“清楚，到现在为止我打的每一个电话，对方都要求先处理他们的事情。我放弃我的周末来弄这件事，却让每个我与之通话的人对我指手画脚，你觉得这很好笑么？”

“我现在的工作处于关健时期，公司对此十分重视，我今天下午要完成它，你还有什么不明白的？”

“在我开始恢复前还有很多电话要打，”雷蒙说。“我们说定星期二恢复你文件的使用，怎么样？”

“星期二不行，星期一也不行，要今天，现在！”斯蒂夫边说边考虑如果说不通这个大脑迟钝的家伙，他该向谁打电话。

“好吧，好吧，”雷蒙说，斯蒂夫还能听到他无奈的叹了口气。“我看看我该怎么让你连线，你使用RM22服务器，对么？”

“RM22和GM16两台。”

“好，很好，我可以绕过一些程序来节省些时间——我需要你的用户名和口令。”

什么？斯蒂夫想，这是怎么了？为什么他需要我的口令？为什么所有IT部门的人都这样？

“你刚才说你姓什么？谁是你的主管？”

“雷蒙派瑞兹。听着，听我说，当你被雇用的时候，必须填一个表格来取得自己的用户名，同时写下密码。我可以在存档中找到这个文件，然后告诉你，好么？”

斯蒂夫考虑了一会儿，表示同意。他拿着电话尽量耐心的等着雷蒙从文件柜中取出文件，最终返回到电话前，斯蒂夫可以听到他在摆弄一堆文件。

“哈，找到了，”雷蒙说，“你写的密码是Janice。”

Janice，斯蒂夫想，是他母亲的名字，实际上有时他会用这个名字做密码，很可能在他填雇用登记表时就用它做密码了。

“是的，是这样。”他承认道。

“那好，我们正在浪费时间。你知道我是真的，你想让我走捷径帮你快速的取回文件，你就必须给予我帮助。”

“我的用户名是s d 下划线 cramer，c-r-a-m-e-r，密码是pelican1。”

“我会把它恢复正常，”雷蒙说，听上去还比较友好。“给我二三个小时。”

斯蒂夫清理完草坪，吃过午饭，到时间便来到他的计算机前，发现他的文件已经恢复了。他很满意自己强有力的说服了那个不太合作的IT小子，并希望安娜听到了他是多么的果断。最好对那个小子或是他的上司表示一下他的满意，但他知道他抽不出时间做这些事情。

克雷格科格伯恩的故事

克雷格科格伯恩（Craig Cogburne）曾是一家高科技公司的销售，业绩良好。一段时间后，他逐渐意识到自己有一种读懂客户的能力，理解对方反对什么，以及利用对方的弱点和漏洞轻松完成销售任务。他开始思考这种才能的其他用途，和那条最终导致他获利颇丰的道路——商业间谍。

这是个紧急任务，不会花费很长时间，也不值得花钱去趟夏威夷，或是塔希提（Tahiti）。那个人雇用了我，他没说客户是谁。当然，不用说也是一些想一下子轻松、迅速地赶上竞争对手

的公司。我的工作是拿到那个叫做心脏支架的小玩意的设计书和产品说明，管它是什么。对方公司叫做双星医疗，以前从没听说过，是一家500强企业，在不同的地方有六个分公司。对于我的工作来说，大公司比小公司容易得多。因为，在小公司里你很可能会被谈话的对方认出来不是自己所声称的那个人，而这种情况就像飞行员说发生空中碰撞一样，可以把你的一切都毁了。

客户发过来一封传真，说是一些医疗杂志上报道了双星医疗正在研究一种全新设计的心脏支架，可能叫做STH-100。由于事情炒得很热，记者们已经替我做了许多前期调查工作，包括我在开始工作前必须知道的事情，这个新产品的名字。

第一个问题：取得可能会看到这个设计的以及研究STH-100的那些人的名字。于是我打电话给接线员："我答应与你们的一位工程师联系，但我记不起他姓什么了，只记得他的名字是以S开头。"接线员说："有两个人，一个叫斯科特亚谢尔（Scott Archer），一个叫塞姆大卫森（Sam Davidson）。"我冒着风险问："哪一个在STH-100工作组？"她不知道，我只好随意选了斯科特亚谢尔，她帮我接通了电话。

对方拿起电话，我说："嗨，我是麦克，收发室的。我们收到一个寄给STH-100心脏支架方案组的联邦快递，应该给谁？"他告诉我方案组长的名字，杰瑞曼德尔（Jerry Mendel），我甚至还让他帮我查到了电话。

我打给曼德尔，没有在。但他的语音留言说他在度假，一直到13号，也就是说他还有一个星期的时间滑雪或者其它什么事情。在此期间，任何人有事的话打9137找米歇尔（Michelle）。太好了，这些信息太有用了。我挂了电话接着打给米歇尔，她接起电话，我说："我是比尔托玛斯（Bill Thomas），杰瑞说我一旦准备好产品说明书就打给你，他想让组里的人看看。你是心脏支架组的，对吧？"她回答是。

现在，我们到了整个布局的攻坚点了。如果她有所怀疑，我就打出预先准备好的牌，我会说是杰瑞让我帮他这个忙的。我问："你们用哪个系统？"

"系统？"

"你们成员组使用哪些服务器？"

"哦，"她说："RM22，组里有些人还会用GM16。"

很好，这正是我需要从她哪里得到的信息，并且没有引起她的怀疑。接下来，为了尽量麻痹她，我尽可能的令语气自然，“杰瑞说你可以给我一个研发组成员的电子邮件列表，”说完，我屏住呼吸。

“当然，这个表太长了，不便阅读，发邮件给你可以吗？”

坏了！任何一个不以GeminiMed.com结尾的邮箱都会带来无比的麻烦。“你能发传真给我么？”

她顺利的应允了。

“我们的传真机坏了，我得问问另一台的号码，一会打给你。”说完，我挂了电话。

现在，你可能认为我被这个问题难住了，其实这只是任务中的一项常规作业。我调整了一下，好让自己的声音令接线员听起来不那么熟悉，接着我打电话对她说：“嗨，我是比尔汤玛斯，我们的传真机坏了，可以往你的机器上发一个传真么？”她说没问题，然后告诉我号码。接下来，我要去他们公司拿走传真，是这样么？当然不。

第一守则：除非万不得已，绝不与当事人见面。如果你只在电话上与之联系，他们很难认出来你。如果他们认不出你，就不能逮捕你。如何给声音带上手铐呢？

过了一会儿，我打回电话问我的传真到了么？“到了。”她说。

“是这样，”我说，“我还得把它发给我们的一个顾问，能帮我发一下么？”她同意了，为什么？你指望哪个接线员能识别出敏感信息来呢？

她把传真发给那位“顾问”的时候，我正做着当天的运动，迈步走向我附近的一家文具店。那个台头标着”Faxes Sent/Rcvd”（发送传真/已接收）的传真应该比我先到吧，不出所料，我走进文具店时，它已经在那里了。6页，每页1.75美元，我付了一张10元钞和一些零钱，就拥有了那个小组的成员名单和邮件列表。

打入内部

好了，现在我已经跟三、四个不同的人谈过话，并往进入公司计算机系统的方向迈了一大步，但在回家之前还有几件事情要做，首先要搞到从外部拨入工程服务器（译者注：某项目组共用的服务器）的电话号码。我再次打到双星医疗让接线员转到IT部门，然后问接电话的人是否能找一个人给予我计算机方面的帮助。他把电话转给别人，我装作对计算机技术一窍不通。“我在家里，我刚买了一个笔记本，需要设置一下，以便能从外面拨入服务器。”

设置很简单，但我耐心地让他一步一步地教我，直到拨入电话号码。他告诉我那个号码，就像说出其它的一些日常信息。然后，我让他等我试一下。没问题。

现在，我已经克服了连接网络的障碍。我拨号进入，发现他们的终端服务器允许拨入者连接到内网上所有的计算机。多次测试后，我偶然发现一台计算机上的来宾账号口令为空。有些操作系统在首次安装时，会指导用户建立一个账号和口令，同时给出一个来宾账号，用户可以对其设置口令或是禁用它，但多数人不懂这一点，或者是嫌麻烦。这个系统可能是刚安装不久，而主人也没花点儿功夫把来宾账户禁用掉。

专业术语

哈希密码（PASSWORD HASH）：对口令进行一次性的加密处理而形成的杂乱字符串，这个加密过程被认为是不可逆的，也就是说，人们认为从哈希串中是不可能还原出原口令的。（译者注：2004年，王小云教授在国际密码学大会上公布了破解HASH函数的关键技术。）

多亏这个来宾账号，我现在访问到了一台运行着旧版本UNIX的计算机。UNIX的操作系统备有一个密码文件，这个文件包含所有有权访问这台计算机的用户的加密口令，也就是一次性加密的哈希密码。经过一次性哈希加密，一个真正的口令，比如“justdoit”，会被加密后的哈希字符代替。在这个案例中，口令被转换成13个字符位的数字和字母。当有人访问计算机时，需要输入用户名和口令以确认身份，这时系统就会对输入的口令进行加密，然后把结果与密码文件中的哈希口令对比，两者如匹配，访问允许。由于文件中的口令是加密的，因此虽然在理论上文件本身对于任何用户都是有效的，但并没有已知的办法能够解密口令。

这真是笑话。我下载了这个文件，运行字典攻击（本书第十二章有更多的攻击方法），发现研发组的一个叫斯蒂文克莱默的工程师，在这台计算机中拥有一个口令为"Janice"的账号。我试着在一台服务器上输入这个口令碰碰运气，如果有效，这不仅会节省我的时间，还会让我少冒些风险。但口令无效。这就意味着我不得不用些技巧来让这个人自己告诉我他的用户名和密码。于是，我一直等到周末。后面的事情，你们已经知道了。周六，我打电话给克莱默，用蠕虫和服务器必须从备份中恢复的理由打消他的怀疑。也许有人要问，他填写雇用登记表时的口令是怎么一回事？我指望他不会记着所有的事，一个新员工要填的表很多，几年之后，谁还会记得呢？而且，即使我在他身上的努力失败，那份长长的名单上还有其他人可以尝试。

利用他的用户名和口令，我进入服务器开始搜索，很快找到了STH-100的设计文档。但我不确定哪些是关键的，于是我把所有的文件传送到"秘点"，中国的一个FTP站点，文件存放在那里不会引起任何人的怀疑，让客户在这堆垃圾里寻找他们的宝贝吧。

专业术语

秘点（DEAD DROP）：很难被别人发现的存放信息的地方。在传统的间谍活动中，秘点可能是一堵墙壁上某块松动的石头。对于计算机黑客来说，一般都是位于遥远国度的互联网上的一个站点。

过程分析

那个我们称之为克雷格科伯恩的人，或是任何像他一样具备熟练社会工程学（不总是以违法行为盗窃信息）能力的人，以上叙述的难题几乎都如例行公事般简单。克雷格的目标是在一台受到保护的企业计算机上找到并下载文件，这台计算机被防火墙和通常所有的安全技术保护着。他的大部分工作如探囊取物般简单。先是假扮收发室的工作人员，声称收到一封不知寄给谁的联邦快递包裹来增加紧迫感，这样他得到了心脏支架研发组组长的名字，这位组长正在渡假，可他却留下了助手的名字和电话--这大大地方便了试图窃取信息的社会工程师。克雷格打给这位助手，谎称响应项目组长的要求来打消她的怀疑。组长不在城里，米歇尔在无法证实他所言属实的情况下，相信了他的话，并把项目组成员名单毫无保留地提供给他。对于克雷格来说，这是一组十分

必要和珍贵的信息。

当克雷格让他发传真而不是使用令双方都方便的电子邮件时，她甚至都没有怀疑。为什么她如此轻易的相信他人？如同许多工作人员那样，她可不想在上司回来时发现她拒绝了一个人的要求，而这个人所做的事是她的上司交待要做的。此外，对方并没有说上司明确批准了他的请求，只是需要他的协助。她之所以还把名单给他，是因为有些人有一种显示自己是团队一员的强烈愿望，而这种愿望使大多数人容易被骗。

克雷格避免了亲自现身的风险，他让对方把传真发到接线员那里，他知道接线员会有帮助的。一般来说，接线员都有着温柔的性格和给人留下良好印象的素养，像收发传真这种在职责范围内的小忙，克雷格可以充分利用。虽然任何知道此信息价值的人看到她发出的信息都会引发警报，但你又如何指望一个接线员能分辨出无害信息和敏感信息的区别呢？

米特尼克信箱

每个人对工作的第一考虑就是完成工作，在此压力下，安全操作规程就放到了第二位并被遗漏和忽略，社会工程师就利用这一点来实施他们的诡计。

克雷格利用了一个从未改变过的默认口令，许多依靠防火墙的内部网络都存在着这种即明显又开放的漏洞。实际上，许多操作系统、路由器和其它产品，包括专用交换机的默认密码，在网上都有提供。任何一个社会工程师、黑客，或是商业间谍，还有那些仅仅是具有好奇心的人，都可以在http://www.phenoelit.de/dpl/dpl.html找到这个默认密码列表，简直令人难已置信，互联网把那些知道从哪里获取资源的人的生活变得如此轻松，现在，你也知道了。

然后，科伯恩竟然让一个行事谨慎怀有戒心的人透露了他的用户名和口令，从而访问到心脏支架研发组使用的服务器。这就如同在公司最严守的秘密上开了一扇门，克雷格可以任意浏览信息并下载新产品计划。

如果斯蒂文克莱默继续他对克雷格的怀疑又会怎样？斯蒂文看来不大可能在他星期一早晨上班前报告此事，而到了星期一已经晚了。这个骗局最后部分的一个关键就是，克雷格先是显得对

斯蒂夫所担心的事情漠不关心，接着换成一付让对方听起来是在帮助对方完成工作的口吻。许多时候，当受骗者认为你是在帮他或是在为他做事情时，往往会放开在其他情况下会坚守的秘密信息。

预防措施

社会工程师一个最强有力的技能就是扭转局面，这你已在本章中看到。社会工程师制造问题，然后魔术般地给予解决，然后从受骗者手中套出访问企业最严守的秘密的通道。你的员工会掉入这个圈套么？设计和实施这样一套防范攻击的安全规程，你会感到棘手么？

培训、培训，再培训……

有一则老故事，一个去往纽约的游客在街上叫住一个人问："我怎样才能到达卡内基音乐殿堂？"那个人回答："练习，练习，再练习。"每个人在社会工程师的攻击面前都很脆弱，而企业唯一有效的防范就是培养和训练员工，给予他们练习的机会，如何认出一名社会工程师。而且，要不断的始终如一的提醒他们在训练中学到的知识，否则很容易忘掉。

企业里的每一名员工人在与不是亲自认识的人打交道时，应具有适度的谨慎和警戒心，特别是访问计算机网络的有关事情要尤为注意。人类天性容易相信他人，但正如日本人所说"商场如战场"，公司在安全防护方面绝不能放松警惕，必须制定安全策略以清楚的区分哪些是不当的操作，哪些符合规程。安全措施不是千篇一律，企业员工通常都有着差别很大的任务和职责，而每个岗位都有着与之相关的漏洞。公司里的每个人都应完成一个基础培训，并加上依据他们的工作程序而设计的培训，以降低员工本人发生问题的可能性。而工作涉及敏感信息或身居关键职位的员工，更应给予专门的培训。

保持敏感信息的安全

如同本章中所讲的那样，当一个陌生人以提供帮助的名义与工作人员接近时，工作人员必须遵循为适合公司文化、业务需要而定制的合适的安全策略。

注：个人认为，并不是所有的企业都需要共享和交换密码，建立一个严格的规则来禁止员工共享和交换机密口令很容易，而

且也更安全，但每个企业必须结合自己的工作环境和安全要点来做选择。

绝不要配合陌生人查询信息、在计算机上键入不熟悉的命令、改变软件设置，或是打开邮件的附件和下载未经检测的程序（这最有可能造成危害）。任何软件程序，即便是那些看上去无碍的程序，也很可能暗藏危险。

有些工作，无论我们的培训做得有多好，时间一长，我们就又粗心大意起来。接着便忘掉了非常时期的培训，因为那时正需要它。你可能认为不要泄露你的用户名和口令是一件无需提醒的事，任何人都知道或都应知道，这是一种普遍的认识。但实际上，每个员工都需要被经常提醒--泄露办公室计算机、家庭计算机、甚至是邮资机的用户名和口令与泄露ATM卡的个人身份识别码一样危险。

有时，在非常偶然的情况下，在有限的环境下，把机密信息透露给别人是必要，甚至可能是十分重要的。为此，制定"永远不要"的绝对规则是不合适的。然而，为特定环境制定相应的安全策略和规程十分必要，员工在非常时期可以把口令透露给别人，但对方必须被授权。

注意对方身份

在大多数机构中，安全规则要囊括所有可能给企业或工作人员带来损失的信息，只能是亲自认识的人，或是十分熟悉对方声音的情况下才能将信息透露。在高度防范的情况下，只有人员亲自在场的要求才被许可，或是通过一个强有力的认证模式，比如通过两个单独的检验条件，像共享密码和时间令牌。数据分类措施也必须指明公司敏感工作部门的信息不要透露给不认识的人或以某种形式担保的人。

注：很难让人相信，即使在企业员工数据库中查询打电话人的名字和电话号码并拨打回去，也不足已保证对方的身份。社会工程师懂得如何把名字放入数据库中和把电话转拨的方法。

那你又该如何处理公司的另外一名工作人员听起来十分合理的要求呢？比如，他需要你们部门的名单和电子邮件列表。实际上，对这种仅供内部使用，且明显没什么价值（这与新产品说明书的价值不可同日而语）的信息，很难对其提升安全意识。一个

主要的解决方法就是，为每个部门指派一个负责处理对外发布信息的人，并给他们安排相应的培训，以使其明白应该遵循的确认程序。

勿有遗漏

任何人都可以对企业哪里需要高级别的安全防护以杜绝恶意攻击的事情夸夸其谈，可我们却经常忽略其它地方，这些地方并不明显，但极易受攻击。在上述的故事中，发传真到公司内部的一个号码似乎比较安全，没什么害处，但攻击者却利用了这一点。从这个例子中应该吸取如下教训：

公司的每一个人，从秘书、行政助理到执行人员和高层管理者都需要进行专门的安全培训，以使他们面对类似的欺骗手段时保持警醒。而且，别忘了看好前门--接线员，通常也是社会工程师的首要目标，必须让他们了解某些来访者和打电话人的骗术。企业安全部门应该建立一个单一的联系点，类似于情报中心，为那些认为自己可能成为社会工程师的攻击目标的员工汇报情况时所用。这样的一个情报中心会提供有效的预警系统，清晰化悄然发生的攻击，从而令任何破坏行动得到及时的控制。

第六章你能帮我吗？

大家在前面已经看到社会工程师如何通过提供帮助来使人上当，他们的另一个惯用伎俩是假装需要别人的帮助，因为我们都会对处于困境的人施与同情，社会工程师便经常的利用这一方法来达到他的目的。

外地人

第三章中有个故事显示了攻击者如何通过对话令对方说出他的员工号码，下面的故事则运用不同的方法得到了相同的结果，并且这个故事还将展示攻击者如何利用这个号码。

硅谷有一家不太知名的全球企业，散落在世界各地的所有销售处和现场基站都是通过WAN——广域网，连接到公司总部。入侵者，一个叫布瑞恩亚特拜（Brian Atterby）的狡猾的活跃分子，他知道入侵一个远程站点的网络总是要比总部的网络容易的多，由于前者的保护措施较为薄弱。

我找琼斯

他打电话到这家公司的芝加哥办公室，找琼斯（Jones）先生讲话，接线员问他是否知道琼斯先生的名字。
"我有他的名字，我正在找，你们那儿有几个叫琼斯的？"
"三个，你找的琼斯在哪个部门？"
"如果把他们的名字念一下，可能我就会想起来了。"
"拜瑞（Barry）、约瑟夫（Joseph）和格丹（Gordon）。"
"是乔（Joe，约瑟夫的昵称），肯定是他，他在，哪个部门？"
"商务拓展部。"
"很好，请帮我转过去好么？"

接线员将电话接通，琼斯接起电话，攻击者说："琼斯先生？嗨，我是托尼，薪金发放专员（译者注：相当于管理工资发放的会计），我们刚刚依据你的要求，把薪金支票存入到你的信联账户上。"
"什么？？？你在开玩笑吧！我从来没这样要求过，我甚至在信联都没有账户！"
"哦，见鬼，我已经转过去了。"

一想到到薪金支票可能转到了别人的账户上，琼斯十分的心烦意乱，并开始怀疑电话另一端的小子是不是有些智力低下。他不知道该说些什么，这时攻击者说："我得看看是怎么回事，薪金发放时要输入员工号码，你的号码是多少？"琼斯告诉了他。

"哦，不，你说得没错，发出请求的人不是你。"攻击者说。他们越来越蠢了，琼斯想。

"这样，我看一下谁负责此事，然后把错误马上改过来。请别担心，下次不会这样了。"

对方向他保证。

一次商务旅行

不久之后，这家公司在得克萨斯首府奥斯丁销售处的系统管理员接到了一个电话。

"我是约瑟夫琼斯，商务拓展部的。这星期我要入住德斯基（Driskill　Hotel）饭店，我想让你帮我建立一个临时帐号，以免除远程拨号才能访问我的电子邮箱。"

"让我再确认一下你的名字，告诉我你的员工号码，"系统管理员说。假琼斯告诉了他，并说："有没有速度很快的上网拨号？"

"请等一下，老兄。我得在数据库中确认一下。"不一会儿，系统管理员说："好的，乔，你的楼牌号是多少？"攻击者对此早有准备，报上了备好的答案。

"好的，"系统管理员对他说："验证通过。"

如此简单，系统管理员确认了约瑟夫琼斯的名字，部门，还有员工号码，针对他的测试问题，"乔"也给出了正确的答案。

"你将使用的用户名与你在公司的一个用户名相同，jbjones，"系统管理告诉他说，"并且我将你的口令初设为changeme"。

米特尼克信箱

不要指望网络安全装置和防火墙来保护你的信息，要注意最薄弱的环节。通常，那就是你的员工。

过程分析

拨几个电话用上15分钟的时间，攻击者就可以访问这家企业的广域网了。有很多这样的企业，都属于我要提及的"软心糖安全"，这个概念最早是由贝尔实验室的两位研究人员提出的，斯蒂夫贝劳文（Steve Bellovin）和斯蒂文切斯威克（Steven Cheswick）。他们用这样的词语来描述这种安全防护："坚硬生脆的外壳，核心却很柔软"，如同M＆M巧克力糖（一种驰名的糖果品牌），两位研究人员说，外壳即防火墙并不足以保证安全，因为一旦入侵者绕开它，内部的计算机系统便不堪一击。大部分情况下，这种保护措施是不够的。

上面的故事符合这个定义，利用得到的拨号和账户，攻击者甚至不用费力去攻击防火墙。而且，一旦他进入内部，内网的大部分系统就十分危险了。由于我我的经历，我知道这种骗局曾在世界最大的软件生产商身上起过作用。依据我的经验，在一个聪明的具有说服力的社会工程师面前，没有人是绝对安全的。

专业术语

软心糖安全：贝尔实验室的贝劳文和切斯威克提出的说法，用以描述一种安全状况。外部防御十分强壮，如防火墙，但其后面的设施却十分脆弱。这个说法来自于M＆M巧克力，这种糖果有着坚硬的外壳和柔软的糖心。

地下酒吧式的安全：知道自己想要的信息在哪里，并且使用一个词或是名称来获得对此信息或计算机系统的访问权的一种安全形式。

地下酒吧式的安全

对于早期的地下酒吧--那些在禁酒令时期提供自酿酒的夜总会，一个顾客需要走到门前敲门，然后门上会打开一个小口，伸出一张冷冰冰的脸。如果来人熟悉情况，他就会说出此地的老主顾（一句"乔让我来的"就可以了），看门的护卫就会打开门让他进来。

这个事情的关键在于知道地下酒吧的位置，门上没有标志，而酒吧老板也不会挂一盏霓虹灯在门口来表示这儿有个酒吧。通常，只要能找到地方就基本可以进入。很不幸，同样的安全措施在企业中广泛存在，这种没有任何保护的安全级别我称之为地下酒吧式的安全。

我在影片中见到过它

这儿有一个例子，来自一部许多人都会想起来的电影。《英雄不流泪》（Three Days of the Condor）中的主角，特纳（罗伯特瑞德福特饰演）为一家与中央情报局签约的小调查公司工作。一天，他吃完午饭后回来发现他的同事们都被枪杀了，他决定找出凶手和真相，同时那些坏人也一直在找他。故事的后面部分，特纳（Turner）设法得到了其中一个坏人的电话号码，但这个人是谁？特纳又如何确定他的在哪儿呢？他很幸运。编剧大卫瑞菲尔轻松的给了特纳一个美国陆军通讯兵的受训背景，使他在电话方面有着丰富的知识和经验。特纳当然知道该如何利用手中的电话号码，在剧本中，那幕场景是这样的：

特纳重新拿起电话拨出另一个号码

叮呤！

女性的声音从电话中传来：CNA，我是科尔曼（Coleman）夫人。

特纳：科尔曼夫人，我是哈罗德托马斯，客户服务CNA202-555-7389，谢谢。

科尔曼夫人：请稍等。（几乎是同时）兰纳德亚特伍德，马里兰州切维柴斯区麦克肯色街765号。

虽然编剧错误地把华盛顿特区的电话区号用到了马里兰州，但我们没必要注意这个细节。关健是弄明白刚才的对话是怎么一回事。

特纳由于有通讯兵的受训背景，他知道如何给电话公司的CNA部门（Customer Name and Address - 客户名称与地址）打电话。CNA是为了方便电话安装员和其他得到授权的电话公司职员而成立的部门，电话安装员拨打CNA并提供一个电话号码时，CNA的服务人员就会报出电话所有者的名字和地址。

愚弄电话公司

在现实世界中，CNA的电话号码保护的十分严密。尽管当今的电话公司最终明白这一点，并不再轻易的泄露此类信息，但在

当时他们却实行着地下酒吧式的安全，那时的安全专家们管这种安全叫做隐晦安全。他们假定任何给CAN打电话并知道其专业用语（如，客户服务CNA555-1234）的人都已被授权得到相应信息。

专业术语

隐晦安全：一种效率低下的计算机安全手段，通过对系统运转细节（协议、算法和内部系统）的保密来达到防范目的。隐晦安全假定可信任成员组以外的人不能接近系统，因此这种安全并不可靠。

米特尼克信箱

隐晦安全在社会工程师的面前毫无用处。在这个世界上，每一个计算机系统至少有一个人在使用。因此，如果社会工程师能够操纵这个使用系统的人，系统的隐晦就没有意义。不用亲自验证或确认，不用提供员工号码，也不用每天改变口令，只要你知道正确的电话号码并听起来可以信任，你就有权得到相关信息。对于电话公司来说，情况并不总是这样，他们还会定期的（至少一年一次）改变电话号码做为仅有的安全举措。即便这样，某个特定时期的号码还是在电话盗打者的圈子里传得很广，他们很高兴利用这个便利的信息资源，并乐于在同行中分享他们的所做所为。在我十几岁习惯盗打电话的时期，拨打CNA我最先学到的手段之一。

在全世界的政府和企业中，地下酒吧式的安全仍然很普遍。它可能是你公司的部门、员工和专业术语，有时连这些也用不着，一个内部电话号码就够了。

粗心的计算机管理者

尽管企业中的许多员工都对信息安全的危险或给予忽视或漠不关心，或是没有这方面的意识，但那些500强企业中计算机中心的管理者应该对安全操作了如指掌了吧，对吧？

不要期望一位计算机中心的管理者--负责公司IT部门的人，会掉入简单、明显的社会工程学圈套，尤其是还带有孩子气的、刚步入社会的年轻社会工程师。但有时，这样的想法是错误的。

收听

在以前，对许多人来说，把无线电调到地方警察局或消防队的频率收听正在进行中的银行抢劫、办公大楼起火、高速追击是一件很有趣的事情。执法部门和消防部门使用的无线电频率，曾经从街角书店的书中就可以查到。现在，在网上就有这些频率的列表，你还可以从Radio Shack（译者注：美国著名电子产品零售商）买到列有地方、郡、州有时甚至是联邦机构无线频率的书。

当然，不只是那些怀有好奇心的人，午夜抢劫店铺的窃贼会收听是否有警车派到附近，毒品贩子要始终关注的毒品缉查人员的行动，纵火犯则通过放火后收听消防队奋力灭火的情况来满足他的变态嗜好。

最近几年来，计算机技术的发展已经使声音信息的加密成为可能。在工程师们不断的找到方法把越来越多的计算能力塞进一块微芯片时，他们也开始制造小巧的加密无线设备，帮助执法部门来防范坏人和怀有好奇心的人窃听。

窃听者丹尼

一个我们称之为丹尼的扫描器爱好者，同时也是位技巧娴熟的黑客，他想看一下自己是否能够染指由安全无线系统顶级生产商开发的绝密的加密软件源代码。他希望通过这些代码了解如何对执法部门进行窃听，同时利用此技术令即便是最强有力的政府部门也很难监视他与朋友的通话。在朦胧的黑客世界中，丹尼这样的人属于特殊的一类，介于无恶意的好奇和完全的破坏之间。他们有着专家般的知识和极易引起麻烦的黑客想法，为了智力挑战和了解技术细节带来的满足感入侵系统和网络。但是他们惊人的电子入侵技术，也仅仅是一种特技。

这些人，这些无恶意的黑客，非法进入别人的网站纯粹是为了有趣并为能够证明自己的能力而感到满足。他们并不偷窃，也没有利用这种手段来赚钱。他们不会破坏文件、中断网络连接，或是摧毁计算机系统。他们的目的就是悄悄地捕获文件拷贝、搜索电子邮件、得到密码，以嘲弄那些网络管理员和对安全负责的工作人员，他们的满足感基本来自于这种胜人一筹的能力。

就这样，我们的丹尼为了满足自己强烈的好奇心并为了对生

产商可能做出的惊人革新一看究竟，他将检验对方高度保护的产品信息细节。不用说，这种产品的设计是受到严密保护的，如同公司其他贵重的财产一样。丹尼知道这一点，但他并不怎么担心。毕竟，这只是一家没什么名气的大公司。但他如何得到软件的源代码呢？

正如我们最后将要看到的，从公司的保安通讯小组中猎取信息很容易，即使这家公司也使用了双因素认证（用户需两种单独的标识来证明身份）技术。这里有一个你可能已经熟悉的例子：当你的信用卡更换日期到了的时候，你需要给发行公司打电话，让他们知道信息卡还在持卡人的手中，并没有被人偷走。信息用卡上会说明在通常情况下要从家打电话，当打电话时，信用卡公司的软件程序就会分析ANI（自动号码认证），并被转到公司的免费电话上。信用卡公司的计算机使用ANI提供的呼叫方号码，与公司持卡人数据库中的号码做比较。公司的工作人员在接电话时，他或她就会看到数据库中显示的客户详细信息。这样，工作人员就知道了电话是客户从家中打来的，这就是一种形式的认证。

专业用语

双因素认证：用两种不同的验证方式对身份进行确认。比如，一个人必须从某个可确认的地方打来电话并知道口令来确认自已的身份，然后工作人员从你的信息中选出某个条目（通常为社会保险号码、出生日期或是母亲的姓氏）来询问你，如果你的答案正确，这就是第二次的验证——基于你应该知道的信息。我们故事中那家生产安全无线电系统的公司，每一名有权访问计算机的职员都有自己的账号和口令，并另外配备一个叫做安全ID的电子小设备，这就是时间令牌。它有两种型号：一种只有一张信用卡的一半大小，但稍厚些。另一种小到可以挂到钥匙链上。

这个特殊的装置由加密技术衍生而来，它的上面有一个显示六位数字的小窗口，每六十秒改变一次。当一位得到授权的用户从外部访问网络时，她首先必须输入她的PIN码和令牌上的数字，依此来确认自己的身份。内部系统一旦予以确认，她就可以输入用户名和口令进行认证。

对于觊觎着源代码的年轻黑客丹尼来说，他不仅要解决用户名和口令的问题（对于经验丰富的社会工程师来说这算不上什么难题）还要绕过时间令牌的检测。攻破基于时间令牌和用户PIN码的双因素认证听起来像是一个"不可能的任务"，但对于社会工程师

来说，这种挑战类似于一个能够占尽对方优势的有着高超观察能力的牌手，再加上一点儿小运气，当他在桌子旁坐下来时，就知道别人口袋里的钱基本已是他的囊中之物了。

冲击堡垒

丹尼先是做准备工作，很快他就得到假扮一个真正的雇员所需的各种信息。姓名、部门、电话号码和员工号码，还有部门经理的姓名和电话号码。现在，是攻击前的平静期。按照计划，丹尼在采取下一步行动前还需要一个条件，而此事他毫无把握：丹尼需要大自然母亲的帮助，他需要一场暴风雪，一个阻止人们去办公室上班的恶劣天气。在南达科他州的冬季，那家生产商的所在地，一个恶劣气候从不会让希望它的人等太久。星期五晚，一场暴风雪到了。雪迅速的转成冰雨，到了早晨路面就会结一层薄薄的冰，十分危险。这对丹尼来说，简直太好了。

他打电话给那家厂商，转到计算机机房，找到一名自称罗杰科瓦斯基（Roger Kowalski）的计算机操作员。

丹尼："我是安全通讯部的鲍伯比林斯（Billings），我现在家中，因为冰雪的缘故我无法开车。我现在需要访问我的工作站和服务器，但我把安全ID忘到办公桌上了，你能帮我拿回来么？或者让别人帮一下忙，然后当我登录的时候给我念一下好么？我的工作任务有一个最后期限，我没有别的办法。而且，我也没办法去办公室，路况太糟糕了。

操作员科瓦斯基："我不能离开计算机中心……"，

丹尼："你自己有安全ID么？"

科瓦斯基："计算机中心有一个，我们保留它是为了操作员应对紧急情况的。"

丹尼："听着，你能帮我这个忙么？我拨号入网的时候，借用一下你的安全ID可以么？路况一能驾车就不用了。"

科瓦斯基："你是谁来着？你的上司是谁？"

丹尼："埃德特伦顿（Ed Trenton）。"

科瓦斯基："哦，我认识他。"

当事情比较棘手时，优秀的社会工程师会多做一些调查工作。"我就在二层，"丹尼说："罗伊塔克（Roy Tucker）的旁边。"科瓦斯基也知道这个人。丹尼接着重新建议他："到我的办公桌取来安全ID很方便。"

丹尼完全断定对方不会听从他的建议。首先，对方不会在当班的时候离开岗位，穿走廊、爬楼梯到大楼的另一边。也不会到别人的办公桌上乱翻一通，打搅别人的私人空间。没错，这个赌注很安全。

科瓦斯基不想对一个需要帮助的人说"不"，当然他也不想擅自做主张而让自己陷入到麻烦中，于是他做了个折中的决定。"我得请示一下，稍等。"他放下电话，丹尼能听到他拿起另一个电话拨打并解释这件事。科瓦斯基这时做出了让人难以理解的陈述（他实际上已经认定了丹尼就是鲍伯比林斯）。"我认识他，"他对他的主管说："他的上司是埃德特伦顿。我们能让他用一下计算机中心的安全ID吗？"

丹尼惊奇地偷听着科瓦斯基对他意乎寻常、意料之外的支持，他简直无法相信自己的耳朵。

又过了一会儿，科瓦斯基拿起丹尼的电话说："我们经理想亲自跟你说话。"然后告诉丹尼经理的名字和手机号码。丹尼打过去又把整个故事重复了一遍，同时又添加了一些工作细节和他的工作为什么有一个最后期限。"如果有人拿回来我的安全ID就方便多了，"丹尼说："我想桌子应该没锁住，它就在左上方的抽屉里。"

"嗯，正好是周末，"经理说："我想你可以用计算机中心的ID，我让值班人员在你拨入的时候给你读一下随机访问码。"然后他把相应的PIN码告诉了丹尼。整个周末，丹尼只需打电话给计算机中心让有关人员念一下安全ID上的六位数字，便随时都可以进入这家企业的计算机系统。

内部任务

当丹尼进入这家企业的计算机系统后，又该怎么办？他如何找到那台放有他想要的加密软件的服务器呢？对此，他已有所准备。许多计算机用户都知道电子公告板形式的新闻组，人们可以把问题贴上来或者回答别人的问题，也有人用它来寻找拥有共同兴趣的虚拟伙伴，如音乐、计算机，或者是其他成百上千的主题。在新闻组站点上发布信息的时候，很少有人会想到这些信息会在网上保留数年之久。比如Google，目前保留着7亿条信息量的存档，某些信息已经有了二十年的历史。丹尼首先访问了http://groups.google.com这个网址，用"无线加密通讯"和那家企业的名称做为关键词进行搜索，结果发现了一条数年前某个职员贴出的

信息，是在这家公司刚开始开发这个产品的时候贴出的，很可能是在警察部门和联邦机构考虑使用加密无线信号很久以前的事了。

这条信息包含了发送者的签名档，其中不仅有他的名字——斯科特普瑞斯（Scott Press），还有他的电话号码，甚至他的工作组名称——安全通讯小组。丹尼发现这个电话后打了过去，这个机会似乎很渺茫。多年后他仍然还在这家公司么？在这个暴风雪的周末他还会在工作么？电话铃在响，一声、二声、三声，一个声音从电话另一端传来，"我是斯科特，"对方说。

丹尼介绍自己是公司IT部门的，从而操纵着普瑞斯（用前几章中大家已熟悉的方法）透露出研发部门所使用服务器的名称，这些服务器的上面可能存有这家企业无线安全产品固件和独有加密算法的源代码。

丹尼越来越接近目标，也越来越兴奋。他期待着那种快感，那种当他完成只有很少人才能达到的目标时所感到的狂喜。然而，他现在还不能放松。虽然由于计算机中心经理的支持，可以随时进入这家企业网络系统，同时也知道了需要访问的服务器。但是，在他拨入时他登录的终端服务器却不能连接到安全通讯小组的系统。一定是有内部防火墙或是路由器保护着研发组的计算机系统，丹尼必须找到其他的办法进入。

接下来的情况需要些胆量，丹尼再次给计算机中心的科瓦斯基打电话抱怨："我的服务器不让连接，我需要你帮我建一个账号来telnet（远程登录）系统。"

既然部门经理已经同意告诉他时间令牌上的访问码，当然这个新的请求似乎也没什么不合理。科瓦斯基在计算机中心的计算机上建立了一个临时账号，然后告诉丹尼不再需要这个账号时通知他，好把它删除。有了这个临时账号，丹尼便可以连接到安全通讯小组的系统了。经过了一个小时的查找，丹尼中了个头彩，他找到了访问研发服务器的漏洞。很明显，系统管理员并没有时刻关注最新的系统远程安全漏洞，但丹尼关注了。

很快地，他就找到那些源代码文件，并把它们远远地发送到一个提供免费存储空间的商业站点。这样，即使这些文件被发现，也不会追查到丹尼。现在只剩下最后一步了：有条不紊的擦去他的痕迹。他在当晚的杰伊里诺（译者注：Jay Leno，著名脱

口秀节目主持人）的节目播完之前完成了这项工作。

丹尼极为得意他的这次杰作，在这次行动中，他从未把自己置于危险之中，这是一次令人陶醉的激情之旅，甚至比滑雪和跳伞都要过瘾。丹尼那天晚上喝醉了，不只是因为威士忌、杜松子、啤酒和清酒，在盗来的源代码文件中逐步地接近那绝密的无线软件时，他完全沉醉于自己的能力和成功感之中。

过程分析

在上面的故事中，骗局的成功归于那家企业的职员过于相信了打电话人表示身份的话语。这种帮助同事解决问题的热心一方面使工作顺利进展并获得更令人满意的合作认可，另一方面却是极易被社会工程师利用的重大漏洞。

在骗局中丹尼使用的一个小技巧值得注意：他在要求别人到他的办公桌上拿安全ID时，不断地说"拿回来"。这个用语经常做为让狗取东西的命令，没人会乐意为别人"拿回来"东西。由于这一点，丹尼更加的断定这个请求不会被接受，于是其他的解决方法便会自然而来，那正是他想要的结果。那个计算机操作员科瓦斯基，在丹尼随便的说出了一个自己碰巧认识的人名后便完全相信了他。但为什么科瓦斯基的经理（一个IT经理）竟然也同意让陌生人访问公司的内网？仅仅是因为这样的求助电话是社会工程师百宝囊中一个强大的说服工具么？

米特尼克信箱

这个故事表明时间令牌或是类似的认证方法并不能抵挡住一个诡计多端的社会工程师，真正有效的防范是一个尽职尽责职员，不仅严守公司的安全守则而且了解别有用心的人是如何影响他人的行为的。

预防措施

在上述所有的故事中有一点似乎经常提到，那就是攻击者从企业外部进入内部的计算机网络时，帮助他的工作人员都没有采取足够的措施来确认对方的合法身份，是否有权访问系统。为什么我会经常提及这一点呢？因为，这的确是许多社会工程师在攻击时所采用的手段。对于他们来说，这是达到目标最简单易用的方法。一个电话就能解决的事，还有必要再花上几个小时寻找技

术上的漏洞么？

对于社会工程师来说，实施这种攻击最有力的手段就是假装需要帮助，这是攻击者经常采用的方法。既然我们不想禁止员工对同事或客户的帮助，因此特定详细的确认程序成为判断任何人是否有权使用计算机或接触机密信息的必要。这样，我们才可以帮助应该帮助的人，同时保护企业的信息资产和计算机系统。安全程序应清楚、详细的说明不同环境下所使用的各种不同的确认方法，第十七章提供这样的一个详细列表，但在这儿首先要考虑一些指南：一个确认对方的好办法就是拨打公司通讯录上的电话，如果对方实际上是个冒名顶替者，那么这个确认电话不是令你找到真正的人（被冒充者，而这时冒名顶替者还给你打着电话），就是可以听到被冒充者的语音信箱，从而你就可以与冒名顶替者的声音做比较。

如果企业使用员工号码确认身份，务必要把员工号当做企业的敏感信息，小心保护，不要泄露。此规则适用于所有的内部识别信息，如内部电话号码、部门单据，甚至电子邮件。在安全培训中应唤起每个人对陌生人的警惕，不要因为对方听起来熟悉内部或可信就认为他是真正的内部人员，仅仅知道内部的惯例或术语不能做为对方的身份不需要用其他方式确认的理由。

安全管理人员和系统管理员不能只注意其他人员的安全意识，他们自己也需要提醒自己遵循守则、程序和操作规程。密码口令等信息绝不能共享，而对时间令牌或其他方式的认证来说，限制共用则更为重要。应该普遍认识到，这类事物的共享会危害到公司整个的系统布署。共享就意味着无责任，如果发生安全事件，或是其他问题时，就分不清是谁的责任了。

正如我在整本书中不断重申的，员工要熟悉社会工程师的策略和方法，仔细的分析对方的要求，考虑把角色扮演做为安全培训中的一个固定内容，以使员工能较好的理解社会工程师的手段。

## 第七章假冒网站和危险附件

虽然有句老话说“不劳而获是不可能的”，但把免费当做幌子进行促销仍是许多商家愿意使用的方法，无所谓合理（“等一下，还有……，现在打电话，我们将免费奉送一套餐刀和一个长柄锅！”）或不太合理（“佛罗里达湿地，买一亩送一亩！”），而大多数人对免费的渴望往往导致忽略了对方的提议和承诺。我们都熟知“顾客当心，出门不换”的警言，但在这里需要注意的是一另句话：“小心具有诱惑力的电子邮件附件和免费软件。”精明的攻击者会想方设法进入企业的网络，比如利用免费礼物对人们的吸引力。下面是几个例子：

### 你不想免费么？

就像病毒从一开始就给人类带来祸害，给医生带来麻烦一样，计算机病毒给其使用者带来同样的苦难。如今，计算机病毒以其巨大的破坏力受到很多人的关注，它们是由计算机破坏者制造出来的。计算机痴迷者逐渐存心不良，计算机破坏者在卖力的炫耀他们是多么的聪明过人。有时他们的行为像是入门仪式，为了给具有老资格和经验丰富的黑客前辈留下印象，他们攒着劲的制造出会带来危害的蠕虫或病毒。一旦这些“成果”破坏了文件，毁掉整个硬盘，并把自身发给成千上万的毫无防备的人，破坏者便会因此而沾沾自喜。如果这些病毒带来的危害足以成为报纸的新闻和网络上的病毒警告，他们便更加得意洋洋了。

有很多文章来描写这些破坏者和他们制造的病毒，还有防病毒的软件程序和专门的安全企业，但我们在这里并不想过多的讨论如何在技术上防范他们的攻击，以及他们的破坏行为，我们的话题将更多的关注他们的远亲——社会工程师。

### 来自电子邮件

你也许每天都能接到不请自来的邮件，有广告还有提供免费品之类的邮件，这些东西你既不需要也不想要。你知道那无非是些投资建议、电器、维生素或旅游打折之类的东西，还有你并不需要的信用卡、可以免费观看收费电视频道的设备、增进健康或改进性生活的方法，等等等等。

但每当这样的邮件从你的电子邮箱弹出来的时候都会引起你的注目，也许是一个免费游戏、一副你喜欢的名星的照片、一个免费日历软件或是用来保护你的计算机免受病毒侵害的便宜的共

享软件。无论是什么，它都会引导你去下载你想去尝试的文件。

所有的这些行为，包括下载从广告邮件中得知的软件、点击一个你从未听说过的网站链接、打开陌生人发过来的附件，都可能会惹来麻烦。当然，很多时候你得到的也正是你想要的，或者运气很差，令你失望和生气，但至少无害。可有些时候，你会碰到计算机破坏者制造的程序。发送恶意代码到你的计算机上只是攻击的一小步，攻击者会诱导你下载完成攻击所需的附件。

注：

有一种在计算机上悄悄运行的程序叫RAT（Remote Access Trojan）——远程访问控制木马，它给予攻击者充分访问你的计算机的权限，如同坐在你的键盘前。最具有破坏力的恶意代码病毒，像爱虫（Love Letter）、SirCam和Kournikiva等等，都依赖于社会工程师欺骗的艺术，并利用人们不劳而获的心理传播。它时常作为一个具有引诱力的邮件附件而出现，像机密信息、免费色情资料，或者一个更加诡诈的方法——一条你可能定购了某昂贵物品的信息。最后这种方法，利用你害怕信用卡可能被消费的心理，令你打开这些危险的附件。

令人震惊的是，有太多的人因此而上当，即使在一次又一次的被告知打开附件的危险性之后。随着时间的过去，逐渐削弱的危险意识，让我们每一个人都易受攻击。

识别恶意软件

另一种恶意软件在你不知道或未认可的情况下进入你的计算机运行，这种软件伪装的很好，甚至有时它会表现为一个word文档或是powerPoint文件，或含有宏命令，它将悄悄的安装一个未经许可的程序。比如，它可能是一个在第六章谈到过的木马。一旦这个软件安装到你的计算机上，它能够将你每一次敲击键盘的情况反馈给攻击者，包括你的口令和信用卡号。

还有两种恶意软件，听起来些难以置信。一种可以把你说的每一句话都传送给攻击者，即使你认为你的麦克风是关着的。另一种更加恶劣，如果你的计算机配有摄像头，攻击者可以利用它捕获在你计算机前发生的任何画面，即便你认为你的摄像头是关着的，无论白天或黑夜。

专业术语

恶意软件：一种危害性的程序，例如病毒、蠕虫，或是木

马。

米特尼克信箱

小心那些提供礼物的伪装者，否则你的公司很可能会遭受与特洛伊城相同的命运。一旦发现可疑迹象，一定要采取保护措施。有些喜欢恶作剧的黑客可能会在你的计算机上运行一些骚扰程序，如弹开你的光驱、最小化你的当前窗口，或者用最大的音量在半夜播放一声尖叫。虽然这样的伎俩没有什么意思，尤其当你完成工作或准备睡觉时，但至少这些恶作剧不会带来真正的损失。

朋友的消息

也许情况会变得更糟，尽管你已经处处小心。想像一下：你已经决定不再冒险，不再从你不知道和信任的站点下载文件，除了那些可靠的站点，如安全焦点(SecurityFocus.com)和亚马逊(Amazon)。你不再点击不知其来源的邮件链接，不再打开陌生的邮件附件，并检查你浏览器的安全标志，以确定你访问的电子商务或交换秘密信息的站点的安全性。

这样，有一天，你收到一封朋友或商业合作伙伴的带着附件的邮件。这封来自熟人的信不会有危险吧？即使有危险，你也知道该找谁承担。于是，你打开了附件……轰！你又中了蠕虫或是木马。为什么你的熟人会这样做呢？事情并不象表面上那样。事实是，进入到某人计算机上的蠕虫会根据所进入计算机上的地址薄，自动的把自身发给地址薄中的每一个人。这样，每一个中了此蠕虫的计算机都会传给其地址薄上的所有熟人，蠕虫就这样不断地繁殖，如同在水塘中掷下一块石头而产生的波纹。

这种手段之所以有效在于它结合了两个方法：一是在没有戒心的受害者中传播，二是以熟人的面目出现。

米特尼克信箱

人类发明了许多奇妙的方法，以改变世界和我们的生活方式。但每一种带来的进步的科技，无论是计算机、电话还是互联网，总会有人利用它做坏事，以满足自己的私欲。目前的科学技术处于这样一种状态，你在收到熟人的邮件之后仍然要确定它是否安全，是否可以打开，这真是一件令人悲哀的事。

主题变奏

互联网时代有一种骗局，可以让你进入你并不想去的站点，这种事情很常见，花样也很多。下面的例子具有代表性，这是一个发生在互联网上的真实故事。

圣诞快乐

埃德加（Edgar）是一个已退休的保险销售商，一天他收到一封来自贝宝（PayPal，提供方便快捷的在线支付公司）的邮件。这种服务对于一个在某地或是某个国家从不熟悉的商家购物时，尤其方便。贝宝会直接把从买家的信息卡中把钱转到卖家的账户。埃德加是一个古董瓶的收藏者，通过在线拍卖公司eBay做过许多网上交易。他经常使用贝宝，有时一个星期就用数次。于是，埃德加对这封2001年圣诞节期间，像是来自贝宝公司的邮件很感兴趣，这封邮件是一封升级他的贝宝账户的奖励邮件。信中写道：

节日问候！贝宝高级用户：

新年将至，贝宝将往您的账户上划入5美元，你只需在2002年1月1日前，到贝宝安全站点确认这5美元是做为升级你的账户信息所用即可。新年新气象，升级您的账户，以延续您在贝宝的记录，同时方便我们以优质的服务继续为您提供有价值的客户服务。立即升级账户并马上接收5美元，请点击：http://www. Paypa1 -secure. com/cgi bin谢谢您使用贝宝和对我们的支持！圣诞快乐，新年愉快！

贝宝

电子商务网站

你也许知道，人们不大愿意在网上购物，即便是亚马逊、eBay，或象老海军（Old　Navy）、塔吉特(Target)、耐克这样的这样名牌公司和网站。从某方面来看，他们的戒心无可非议。如果你的浏览器使用现在的128位加密标准，那么你从计算机上发往任意一个安全站点的信息都是经过加密的。这些数据经过大量的努力理论上可以被解密，但更可能的是在正常的时间内无法解密，除非是国家安全部（但谁也没听说过，国家安全部对盗窃美国公民的信息卡号以及谁定购了色情录像或情趣内衣感兴趣）。

这些加密信息实际上可以被任何有时间有才智的人所破解。但是，许多电子商务公司把他们的客户信息未经加密的存储在数据库中，在这种情况下，再去耗费巨大的精力去破解一个信用卡号会是多么的愚蠢。更糟糕的是，有许多使用特定SQL数据库软件的电子商务公司都会犯这样的错误：他们从未改变过数据库系

统管理员的默认口令。他们安装数据库时，系统口令默认是空口令，于是它就一直空着。所以，这个数据库里面的内容，对于互联网上任何尝试连接这个数据库服务器的人都是唾手可得的。

这些站点始终都处在被攻击并且信息会被窃取的危险下，而无需复杂的手段。另一方面，那些不愿在网上购物的人担心他们的信用卡信息被盗。但他们却不在意去真实的商店购物，吃午饭、晚饭，甚至去偏僻街道的小酒馆等一样可以用信用卡付费的地方，即便这些地方总是有人偷取信用卡的收据，有时收据还会从垃圾箱中被人找出。还有一些道德败坏的店员服务生会偷偷记下你的名字和卡号，或使用很容易就在网上买到的盗卡装置，来存储在它上面刷过的信用卡数据，以备日后使用。

在线购物有些冒险，但也可能和在真实的商店购物一样安全。当你在网上使用信用卡时，信用卡公司为你提供相同的保护。如果发生欺诈性收费，你的账户只会损失头一笔交易的50美元。因此我认为，对网上购物的恐惧只是另一种错误的担心。

埃德加没有注意到邮件中的几个不对劲的地方，如抬头的分号，混乱的用词（我们以优质的服务继续为您提供有价值的客户服务）。他点击了链接，输入姓名、地址、电话号码和信用卡等信息，然后静静地等待5美元的到来。但他等来的只会是一堆他从未购买过的商品账单。

过程分析

埃德加被互联网上司空见惯的骗局所欺骗，这种骗局有多种形式，其中一种（详见第九章）有着与真正网站一样的界面，看起来真实可信。不同之处在于冒充的页面不会到达用户真正想访问的系统，而是会把他的用户名和口令发给黑客。埃德加被骗了，对方注册了一个域名为paypal-secure.com的网站，看上去如同贝宝的一个安全页面。当他在这个页面输入个人信息时，黑客们便得逞了。

米特尼克信箱

当没有安全保证时，无论什么时候访问一个需要输入个人信息的网站时，一定要确认当前链接是可信和加密的。更需注意的是，不要顺其自然地点击对话框中的"yes"，尤其是有安全提示的对话框，比如无效、过期或废除的数字证书的提示。

变奏之变奏

究竟有多少多种方法可以骗取人们在假冒的网站输入他们的机密信息？我不认为大家对此有一个统一的答案，但无疑是越来越多。

不明链接

一种常见的手法：发送一封具有诱惑力的邮件，提供一个链接。它并不会带你到想去的站点，它只是看起来像那个的站点的链接。另一个已经在互联网上应用的例子是，用paypa1模仿paypal。

乍一看来，像是贝宝的域名。即便受害人注意到这一点，他也可能会以为只是一个文本上的小错误，把1当成l了。而谁又会立刻注意到那是一个数字1而不是小写的L呢？就这样，有很多的人失去了信用卡上的钱，而这个诈骗手段得以继续。假冒网站做的跟真得一样，当人们访问时，便轻率地输入他们的信用卡上的信息。建立这样一种行骗的机制，攻击者只需注册一个用来冒充的域名，发出电子邮件，然后等待那些傻鸟们上钩。

2002年，我收到一封标着来自Ebay@ebay.com的邮件，很明显这是一个群发性质的邮件。见图8.1，（译者注：我的电子书中看不到这张图。）这样的链接应该注意。

-------------------

亲爱的eBay用户，很明显您的eBay账户被第三方所影响并违犯了我们下面的用户协定条款：

4.招投标

用户如果通过固定价格或成为最高价竞买人，并经销售方同意，则有义务与销售方一起完成此项交易，否则此项交易会被本协定或法律终止。

您之所以收到此通知是因为您当前账户服务的中断引起了我们的注意，eBay方面需要立刻验证你的账户，请验证您的账户以免账户被封。点击此处验证你的账户——http://error ebay.tripod.com商标设计和标志为各自拥有者所有，eBay以及eBay图标为eBay有限公司的注册商标。

-----------------

点击这个链接的人会来到一个很像eBay网站的页面，设计精美，带有eBay的图标，令人可信。而且，如果点击页面上的"浏览"、"出售"等一些导航链接，可将访问者带到真正的eBay站点。页面的右下角也有一个安全的图标，为了防止精明的用户发现马脚，仿造者甚至使用HTML加密来掩盖用户信息的发送地。

这是一个极好的基于计算机进行社会工程学攻击的例子。然而，它也有着一些漏洞。内容上文笔较差，尤其是在最后一段的开头"您之所以收到此通知"，这即拗口也用词不当（实施这些骗局的人才不会雇用一个专业编辑人员来修饰这些内容）。此外，任何一个认真的人都会对eBay索取访问者的贝宝账户信息感到怀疑，eBay有什么理由能向用户索取用户在另外的公司中注册的私人信息呢。

而且如果对于互联网很熟悉的人来说，很可能会发现这个链接并不是eBay的域名，而是tripod.com（一个提供免费主页的网站），这无疑是一封非法的邮件。然而，我打赌还是会有很多人在这样的页面上输入他们的个人信息，包括信息卡号。

注：为什么人们可以注册欺骗性和不合适的域名？现行的法律和互联网政策规定，任何人都可以注册任何未经使用的网站名称。有些公司进行维权以抵制那些冒充者，但结果并不理想。通用（美国著名汽车公司——generalmotors.com）对一个域名为fuckgeneralmotors.com的网站提出诉讼，通用败诉。

## 保持警觉

作为互联网的个人用户，我们所有的人都应该保持警觉，当键入个人信息，如口令、账户或PIN码等信息时，要对目前情况有清醒的认识。你的熟人当中，有多少人能保证他在浏览的页面是安全页面？你公司的员工又有多少人知道该如何做？

每个使用互联网的用户都应该认识那个经常出现在网页上的像一个小挂锁样的图标，当挂扣合上的时候，站点则是安全的。如果挂扣打开着，或是就没有挂锁图样，这个站点就不能被确认是可信的，在上面传送的任何信息都可能处于危险之中（信息未被加密）。

然而，一个危及计算机管理员权限的攻击者可能会更改操作系统代码，甚至为其打上补丁，以掩饰计算机已受到攻击的真相。比如，可以绕过浏览器中的程序对显示某站点的数字证书是否失效的检测。再比如，系统可能会被植入rootkit，安装一个或多个很难检测出来的系统级别的后门。

安全连接可以保证站点的真实性，并对传输的信息进行加密。因此，一个攻击者便无法利用他拦截的信息。可以信任一个已经使用加密连接的站点么？不，因为这个网站的站长并没有随时为网站打上必要的安全补丁，因此不能假定任何安全站点都可以对攻击免疫。

## 专业术语

后门：在用户不知道的情况下进入用房计算机的一个隐蔽入口。编程人员在开发软件时，也会用其来进入程序以解决问题。安全超文本传输协议（HTTP）或安全套接层协议（SSL）提供一个使用数字证书的自动机制，，不仅可以加密发送到远端站点的信息，还可以对其进行认证（保证所连接的站点是真实可信的）。然而，这种保护机制对于那些疏于检验地址栏中的网址是否为他们想访问站点的用户是无效的。

还有一个极容易被忽视的安全问题，弹出类似这样的消息框："此站点非安全站点或安全证书已过期，您是否还要继续访问？"许多互联网用户并不清楚它的具体含义，于是他们直接点击"确定"或"是"来继续他们的访问，而没有意识到可能已处于危险之中。

警告：在没有使用安全协议的站点上，一定不要输入个人的敏感信息，如地址、电话、信息卡号或银行账号，或者是任何你不想泄露的私人信息。

托马斯杰佛逊（译者注：Thomas Jefferson美国第三任总统，《独立宣言》的起草人）说过，保持自由需要"永远的警惕"。在一个视信息为流通货币的社会，要保护个人隐私和安全同样如此。

了解病毒

一个对病毒软件的特殊提示：不仅是对企业内网的用户，而且对每一个计算机用户都是必要的。不要只是把防病毒软件装在机器上，还要让其时刻运行（许多人不喜欢这样做，因为会降低计算机的性能）。

另外一个需要谨记的是：保持病毒库的更新。除非你的企业负责为每个员工更新软件和病毒库，否则自己一定要承担起下载最新病毒库的义务。我个人建议每个人都对防病毒软件的更新功能进行设置，以使软件可以每天自动更新病毒库。

专业术语

安全套接层协议：网景开发的用于互联网上客户与服务器端的安全认证协议。经常性的更新病毒库可以基本保证计算机的安全性，但这并不足以完全保证安全，还有一些病毒或蠕虫是防病毒软件公司未知的，因此相应的保护程序也就没有发布。

所有有着远程访问权限的用户，至少要在笔记本电脑或家用电脑上升级防病毒软件和防火墙。老练的攻击者会从整个系统中

寻找到最弱点而发起攻击，因此需要时常提醒那些有着远程访问权限的用户，激活防病毒软件、升级他们的防火墙是共同的安全防范责任，因为你无法指望一个工作人员、主管人员、销售人员，或其他IT部门的人会时刻记得如果他们的计算机没有保护而发生的危险性。

除此之外，我还强烈推荐不常使用但的确重要的防特洛伊木马的软件。在写作这本书期间，已经有两个为人所熟知的防木马程序，The Cleaner(www.moosoft.com)和Trojan Defense Sweep(www.diamondcs.com.au)。

最后，对于那些没有在企业网关上做危险邮件扫描的公司来说，可能是最重要的安全提醒：由于我们习惯于忘记或忽略那些与完成工作不直接相关的事，因此需要反复地以不同的方式提醒员工，不要打开陌生邮件的附件。管理部门也要提醒员工激活防病毒和防木马软件，以防范那些看似可以信任但实则会带来危害的邮件。

第八章利用同情、内疚与威胁

和在15章中讨论的一样，社会工程师利用心理影响引导目标答应他的请求。熟练的社会工程师擅长于刺激情感，比如害怕、兴奋或内疚。他们利用心理自动触发机制，使人们未经分析就响应请求。

我们想让自己和他人都避免陷入困境，正因为如此，攻击者可以利用人们的同情心，让他的目标感到内疚，或者把威胁当成武器。

下面是一些如何利用情绪的热门课程。

电影制片厂的访客

你有没有注意过一些人是怎样溜进有守卫的地方（比如，会议室、私人派对或者图书发布会），而没有被询问是否有入场券或通行证？

同样，一个社会工程师可以在你没有想过可能性的地方谈论他的方法——就像下面这个电影行业的故事一样。

电话响了

“罗恩·希亚德（Ron Hillyard）办公室，我是多罗茜（Dorothy）。”

“多罗茜，你好，我叫凯尔·贝拉米（Kyle Bellamy）。我刚刚加入动画开发部成为布莱恩·格拉斯曼（Brian Glassman）的职员，你们对这里的事情很了解吧。”

“我想，我没有在其它部门工作过，所以我也不是很了解，我能帮你做什么？”

“说实话，我觉得自己有点笨，今天下午为稿件会议约了名作家过来，但我不知道该和谁说让他进来。布莱恩办公室里的人都非常好,但是我不想再麻烦他们教我这件事我该怎么做，那件事我该怎么做,就像我刚刚从大学出来找不到去洗手间的路。你明白我的意思吗？”

多罗茜笑了。

“你可以和安全部门的人说，拨号7，然后6138。如果你联系上了劳伦（Lauren），告诉她多罗茜说她能够帮助你。”

“谢谢，多罗茜。如果我找不到男洗手间，我会再打电话给你！”

他们都为这个想法暗自发笑，然后挂了电话。

大卫·哈罗德（David Harold）的故事

我热爱电影。当我搬到洛杉矶时，我以为我可以和各种各样的电影商业人士见面，他们会邀请我参加聚会并在摄影棚里吃午饭。好，我在这里已经一年了，现在26岁，最近的一次是在环球电影公司遇到了从菲尼克斯和克里夫兰（译者注：均为美国城市）来的一些好人。所以最后我开始记录电话号码，如果他们不邀请我，我就邀请我自己。我就是这样做的。

我买了一份洛杉矶时报并花了几天时间阅读了里面的娱乐专栏，写下不同电影公司的制片人的名字。我首先确定了一个偶然发现的大型制片厂，然后打电话给接线总机，请她转接我在报纸上找到名字的这个制片人。接线员的声音很亲切，我很幸运，如果是一个只在那里盼望着被提拔的年轻女孩，她也许不会给我时间。

然后是多罗茜，她就像是在接待一只迷路的小猫，她很同情被新工作打击了的新人。我肯定很好的触动了她，当你去骗人的时候，他们可不是每次都会给你比你想要的更多的东西。出于同情，她不仅给了我一个安全部门的人的名字，还说我可以告诉那位女士多罗茜希望她帮助我。

当然我计划过无论如何要利用多罗茜的名字，劳伦都没查找我提供的名字是否真的在员工数据库里就信任了我，这让我的目标更好实现。

当我那个下午开车进入大门时，他们不仅把我的名字放到了访客名单里，还为我准备了一个停车位。我在内部餐厅吃了一顿迟了的午饭，然后在这个地方散步直到一天结束。我甚至偷偷摸摸地到了几个摄影棚，看他们拍电影直到7点才离开。那是我经历的令人激动的一天。

过程分析

每个人都曾是新员工。我们对上班第一天的事情记忆犹新，尤其是当我们没有经验，对工作不熟练的时候。所以当一个新员工求助时，他会希望很多人——特别是登记处的人——可以记得他们自己是个新人时遇到困难的感觉并伸出援手。社会工程师了解这些，他知道可以利用目标的同情心来办到。

我们让攻击者轻易地进入我们公司的工作间和办公室实施他们的计划，即使在入口处有守卫并对每一个非员工实行签名程序，任意变化一个在这个故事里使用的诡计，都能让一个入侵者获得一个来宾的认证并光明正大地进入。如果你的公司要求访客被陪同呢？这是个好规定，但是它只在这种假设下才有效——你的员工们真正尽责的拦住任何有或没有访客认证的人并询问他，然后如果对回答不满意你的员工们会联系安全部门。

攻击者进入你的公司获取敏感信息，这对他们来说很容易。

当今世界，恐怖分子攻击的威胁笼罩着我们的社会，比陷入危险中的信息多得多。

“现在就做”

不是每一个使用社会工程学策略的人都是精练的社会工程师。任何掌握公司详细内部信息的人都变得危险，即使任何公司的经理对员工的所有个人信息文件和数据库进行限制（当然，大部分公司都会这样做），危险依然存在。

当不培训员工如何防御社会工程学攻击时，心意已决的人，就像接下来的故事里那位被抛弃了的女士一样，会做出一些大多数老实人认为不可能的事情。

道格(Doug)的故事

总之，和琳达(Linda)的事情不是很顺利，当我看到艾瑞(Erin)时，我就确定她是我的唯一。琳达是，像是，有一点……好吧，有些不确切，不稳定，当她烦恼时她会不经过大脑就行事。

我尽量温和地告诉她必须从我家搬出去，并且帮她整理东西，甚至让她拿走了几张属于我的Queensryche CD。等她一走我马上到五金店买了一把新的Medico锁，把它装在了前门并在当天晚上锁好。第二天上午我打了一个电话给电话公司，让他们更改我的电话号码，并对其保密。

我可以自由地追求艾瑞了。

琳达的故事

我准备离开了，无论如何，那时我还没有作出决定。但是没有人会喜欢被抛弃的感觉。所以只有一个问题，我该怎样让他知道他有多么负心？

想都不用想，他肯定是有了别的女孩，不然不会这样仓促地和我分手。所以我只要稍等一下，然后在晚上很晚的时候开始打电话给他。你知道的，在这段时间他们最不想接电话。

我等到第二个星期才在星期六的晚上11点钟打电话给他，可是他更改了他的电话号码，新号码又没有在电话表里列出来，这正证明了他是一个SOB（译者注：son of a bitch）。

没有关系，我开始在一些文件里四处寻找，那是我在辞去电话公司的工作之前设法带到家里的。就是它——我保存的一张维修票，道格的电话线路有一次出现了故障，这上面列出了他的电话线路。看吧，你可以尽你想要的修改你的电话号码，但你的电话线依然连接在你的房子和电话公司的中继局之间，接通着电话总机办公室(Central Office，或者说CO)。电话线路的设置被这些接通着线路的号码所确认，如果你知道电话公司是怎么样做这些

事情的，像我做的那样，找到电话号码只需要获得目标的电话线路设置。

我有一张这个城市所有CO的列表，里面有他们的地址和电话号码，我找到了我以前和道格这个负心汉住的地方附近的CO号码，然后打了过去，但是没有人接。转接员在你需要他的时候在哪里？足足用了20分钟我才计划好，开始打电话给附近的其他CO，最终锁定了一个人。但是他太远了并且他可能坐在那里什么事都不做。我知道他不会按照我想的去做，但是我已经有了计划。

“我是琳达，维修中心，”我说，“我们遇到了紧急情况。一台医疗机构的服务器当机了。我们使用技术手段尝试重新启动服务器，但是找不到问题所在。我们需要你马上开车到韦伯斯特(Webster) 的CO，看我们离开电话总机办公室能否拨通。”

然后我告诉他，“当你到那里时我会打你电话的。”因为我当然不能让他打电话给维修中心找我。

我知道他不愿意离开舒适的电话总机办公室，穿得厚厚实实的，擦掉挡风玻璃上的积雪，深夜在烂泥地上开车。但这是紧急事件，他没理由说自己很忙。

当我四十分钟后在韦伯斯特的CO里见到他时，我告诉他检查29线2481路，然后他热情地检查了，并说，是的，线路是通的。当然这我早知道了。

所以我说，“好的，我需要你进行LV（line verification线路排查）。”那需要他确认电话号码，他打了一个重复号码给电话拨打者的特殊号码就做到了。他不知道这是个未列在电话表里的号码，或者是这个号码刚刚被修改过。所以他按我要求的做了，并且展示了他的线路工人的测试设置。很好，所有的事情像有魔力一般完成了。

我告诉他，“好的，故障肯定被排除了。”就像我一直都知道这个号码一样。我感谢了他并告诉他我们要继续工作，然后说，晚安。

米特尼克信箱

一旦一个社会工程师了解了目标公司的内部工作流程，用这些信息认识一个正式员工将变得相当简单。所有的公司都需要预防这些来自现在或以前的别有企图的员工的社会工程学攻击。后台检查可以帮助查找有这些行为倾向的人。但是在大多数案例中，发现这些人是非常困难的。在这些案例中唯一合理的安全措施就是执行并审核身份验证程序，包括员工身份和之前有无透漏公司的内部信息给任何人。

道格试图通过一个未公布的电话号码在我面前隐藏起来的故事到此为止。

好戏开始了。

过程分析

这个故事里的年轻女士之所以能获得她想要信息来实现她的复仇计划，是因为她拥有内部知识：那些电话号码、程序和电话公司的行话。有了它们她不仅可以找到一个新的、未公布的电话号码，而且可以在冬季的晚上，让一个电话转接员为了她而穿过整个城镇。

“这是比格(BIGG)先生想要的”

一个流行的非常有效的威胁方式——因为它太简单了——利用权威来影响人们的行为。

只是CEO办公室助手这个名字就很有价值。私人侦探，甚至猎头公司都始终在做这些事情，他们打电话给接线员，说他们想要联系CEO的办公室。当秘书或者助理经理回应时，他们就说他们有一个文件或者包裹给CEO，或者说他们发送了一份email附件，她能把它打印出来吗？或者他们会问，传真号码是多少？顺便问一下，你叫什么名字？

然后他们打电话给下一个人，说，“比格先生办公室的琼尼(Jeannie)要我打电话给你，他说你能帮我。”

这个技巧是打电话时略提权威人士以示相识而提高自己的身份，它通常是个惯用的方法，通过影响目标让他相信攻击者与权威人士有联系而迅速建立友好关系，大多数目标对这些人有好感，因为他们认识他认识的人。

如果攻击者着眼于获取高度敏感的信息，他可以使用这些方法激起受害人有用的情绪，例如害怕和上司之间陷入麻烦。下面是一个例子。

斯科特(Scott)的故事

“斯科特·艾布拉姆(Scott Abrams)。”

“斯科特，我是克里斯多佛·道布瑞 (Christopher Dalbridg)，我刚刚和比格雷(Biggley)先生结束通话，他有些不高兴。他说他10天前发了一条短信给你，想要你把市场调查报告拿给我们分析。但我们没有拿到任何东西。

“市场调查报告？怎么没有人和我提过，你是哪个部门的？”

“我们是他请来的顾问团,我们已经落后于预定计划了。”

“听着，我在去开会的路上，告诉我你的电话号码……”

听上去攻击者现在真的有些失望：“你想让我告诉比格雷先生

吗？！听着，他希望明天早上拿到我们的分析，我们不得不整晚都为它工作。现在，你希望我告诉他我们不能完成，因为我们没有没有从你那里拿到报告，或者你想亲自告诉他呢？”

一个生气的CEO可以摧毁你的一个星期，目标可能会决定在去开会之前较好的解决这些事情。再一次，社会工程师按下了正确的按钮获得了他想要的回应。

过程分析

如果一个人在公司里地位相当低，通过提及权威人士工作的威胁方式很有效，利用重要人物的名字不仅可以消除正常的不愿和怀疑，而且经常让人热情的满足要求。当你认为你帮助的这个人是重要的或有权势的，自然会希望自己变得更加有用。

社会工程师知道，虽然利用高层人士的名字会很有效，但是对小公司使用这种骗局要谨慎：攻击者不能他的目标有和商业副总裁交谈的机会。“我发送了一份产品销售计划给你，那个人跟我说的。”能轻易的引起这样的回答“什么销售计划？什么人？”这将导致公司发现自己被攻击了。

米特尼克信箱

威胁可以引起对惩罚的畏惧心理，使人们合作。威胁也可以引起人们对困境的畏惧心理或者害怕失去新的提升机会。

必须培训员工当安全受到威胁时，质疑权威不但是可以接受的而且是合理的。信息安全培训应当包括教育人们怎样通过友好的途径质疑权威，而不会破坏关系。此外，公司上下都应该支持这些行为。如果一个员工不支持不考虑身份地质疑权威，正常的反应是停止挑战——正好和你想的相反。

社会保险总署(Social Security Administration)了解你的哪些事情

我们喜欢认为政府机构把我们的信息保护得很严密，只有可信的人才能知道。事实是甚至联邦政府都不像我们想象的那样对入侵免疫。

梅林(May Linn)的电话

地点: 社会保险总署区域办公室

时间:星期四的早晨, 上午10:18

“三号Mod,我是王梅林。”

电话另一端的声音听上去像是在道歉，几乎有些羞怯。

“王女士，我是艾伦戴尔·亚瑟，审查中心办公室。我能叫你‘梅’吗？”

“是‘梅林’”她说。

“好的，是这样的，梅林，我们这里来了个新人，他至今还没有电脑，马上他要有一个优先的任务，他就用了我的电脑。我们属于美国政府，我们大声的抱怨，但他们说他们的预算里没有足够的钱为这个人买一台电脑。现在我的上司认为我拖欠了工作并不想听到任何借口，你知道吗？”

“我懂你的意思，好的。”

“你能帮我快速查询一下MCS吗？”他说道，用到了查询纳税人信息的电脑系统的名字。

“当然，你要查什么？”

“首先我需要你对约瑟夫·詹森进行一次阿尔法查询(alphadent)，DOB是7/4/69。”（阿尔法查询的意思是在电脑里按字母顺序查询纳税人的名字，通过生日来确认身份。）

在简短的停顿后，她问道：

“你需要知道什么？”

“他的账户号码是多少？”他说，用到了社会保险号码的内部称呼。她把它读了出来。

“好的，我需要你对那个账户号码进行数据列表(numident)。”打电话的人说。

数据列表是请求她把纳税人的基本数据读出来。梅林回答了纳税人的出生地点、母亲的名字和父亲的名字。当她同样告诉他发行卡的年月和发行它的区域办公室时，打电话的人有耐心的听着。

下一步他请求进行一次DEQY(显然“DECK-wee”是“详细收入查询”的简写。)

DEQY的请求得到了这样的回应，“哪一年的？”

打电话的人回答，“2001年。”

梅林说，“总计190,286美元，户头是詹森微技术公司。”

“还有其它收入吗？”

“没有。”

“谢谢，”他说，“你真是个好人。”

然后他试着和她商量当他需要信息并且不能使用他的电脑的时候能获得帮助，他再次使用了拿手的社会工程学欺骗，试图和同一个人保持联系，避免每次都要寻找新的目标。

“下个星期不行。”她告诉他，因为她要去肯塔基州参加她妹妹的婚礼，在其它的时间她可以帮他，只要她办得到。

当她挂上电话时，梅林感觉很好，因为她为一个未被赏识的公务员提供了帮助。

基思·卡特(Keith Carter)的故事

从电影和畅销犯罪小说里可以得出结论，私人侦探缺乏道德规范，热衷于窥探人们的隐私。他们的行为违反了法律，就差被逮捕了。真相当然是，大部分PI（译者注：private investigator缩写，私人侦探。）的生意运作完全合法。自从他们中许多人开始在他们的工作中宣誓遵守法律，他们就已经完全知道什么是合法的，什么是不合法的，大部分人不会想越过这条线。

这里，仍然有例外。一些PI——比一些更多——所做的确实和犯罪小说里塑造的那些家伙一样。这些人在交易中充当信息经纪人是很出名的，一个要违反法律的人的教养有限。他们知道如果走捷径就可以更快更好地完成任何任务。这些捷径可能严重触犯了法律，那将使他们在高墙下度过数年的时光，不过似乎不能阻止一个肆无忌惮的人。

高消费阶层的PI——这些人在城镇高价出租屋里设计出独特的办公套房——不亲自做这些事情，他们只是雇用一些信息经纪人为他们工作。

我们称呼这个人为基思·卡特，一个不受道德规范限制的私人侦探。

一个典型的案例是:“他藏钱的地方在哪里？”或者有时候是:“她藏钱的地方在哪里？”有时候是一个有钱的女士,想知道她的丈夫把她的钱藏在哪里(虽然为什么一个有钱的女人曾经和一个家伙结婚是一个谜,但这不是基思·卡特现在想知道的,因此没有去找一个很好的答案)。

这个案例里的丈夫名字是乔·詹森，他把钱藏了起来。他“是一个非常聪明的人，他从他妻子家族借了一万美元创建了一家高科技公司，发展成了上亿美元的公司。”按照她的离婚律师所说，他做了一件高难度的事情隐藏了他的资产，这位律师想要一份完成的资产报告。

基思首先确定他的起点是社会保险总署，目标是他们关于詹森的文件，像这样的情形，那里装着非常有用的信息。有了相关信息的帮助，基思可以伪装成目标让银行、经济公司和风险投资公司告诉他任何事情。

他的第一个电话打给了本地区域办公室，使用了任何公众都可以使用的一个的800号码，这个号码列在了本地电话本里。当办事员在线时，基思要求连线产权局的人。等待了一会儿，然后有了声音。然后基思变换了身份,“你好，”他说，“我是格热格瑞·亚当斯(Gregory Adams)，329区域办公室。听着，我在设法联系一个产权调停者操作一个尾数为329的账户号码，我从传真机那里得到的这个号码。”

“那是2号Mod。”这个人说，他查到了号码并告诉了基思。

下一个电话他打给了2号Mod（译者注：上文中说的是三号Mod，不知道为什么）。当梅林响应时，他更换了角色，成了审查中心办公室的一名进行常规审查的工作人员，碰到了问题，他的电脑不得不给别人使用。她把他要找的信息告诉了他，还同意在他将来需要帮助时找她帮忙。

过程分析

是什么使得利用员工的同情心如此有效？在这个故事里，别人用了他的电脑然后“我的上司对我不满了”。人们并不经常表达他们的情感，当他们这样做时，可以使目标再一次失去对社会工程学的本能防御。“我遇到了麻烦，你能帮我吗？”的情感策略是赢得这一天用到的所有东西。

不安全的社会

难以置信，社会保险总署把他们全部的程序操作手册放到了网上，这些信息里有很多对他们有用，但同样也对社会工程师有用。它包含了缩写、术语和怎样请求你想要的东西的指令,就像这个故事里描述的那样。

想要知道社会保险总署的更多内部信息？只要在Google里面搜索或者在你的浏览器里输入下面这个地址：http://policy.ssa.gov/poms.nsf/。除非这个机构已经阅读了这个故事并在你阅读这些以前移除了这个手册，你可以找到在线使用说明，它甚至详细地给出了哪些数据SSA办事员可以提供给执法部门。实际上，那一部门包含了任何可以使SSA办事员相信他来自执法部门的社会工程师。攻击者不能成功的从一个接到审查中心的电话的办事员那里获得这些信息。基思的攻击方式仅仅是使用一些公众难以获得的电话号码，接听的人因此认为打这个电话的人都是内部人员——另一个地下酒吧式安全的例子。协助此次攻击的元素如下：

知道Mod的电话号码。

知道他们使用的术语——阿尔法查询、数据列表和详细收入查询。

假装来自审查中心办公室，那是每一个联邦政府员工都知道的有很大权力的政府研究机构。这给了攻击者一个权威的光环。

一个有趣的事实是：社会工程师似乎知道怎么样进行请求，让一个从来没有想过“你为什么打电话给我。”认为这个电话来自一些完全不同的其它部门的人，可以建立更多的理解。也许他只是想帮助这个打电话的人，好让单调的日常工作能停顿一下，受害人不会去想这个电话有多么不寻常。

最后，这个故事里的攻击者，没有满足于这些到手的信息，他还想要和目标建立联系好让他可以有规律的打电话来。他可以使用普通的同情心攻击策略——“我把咖啡撒在键盘上了。”可是，那在这里不适用，因为一个键盘可以在一天里面更换掉。

因此他使用了这个别人用了他的电脑的故事，他可以适当地将这些扩充：“是的，我想他在昨天就会有一台他自己的电脑，但是一个人进来和另一个家伙进行了一些交易把它给换了。所以这个爱开玩笑的人仍然出现在我的办公室里。”等等。

我很可怜，我需要帮助，像有魔力一般有效。

一个简单的电话

攻击者的一个主要障碍是让他的请求看上去很合理，就像是受害人在日常工作中碰到的常规请求，这些对受害人而言并不陌生。和一生中的其他许多事情一样，进行合理的请求有时候是个挑战，但是接下来，它就会变成小菜一碟。

玛丽·哈里斯(Mary Harris)的电话

日期/时间：星期一，十一月23日，上午7:49

地点：麦斯拜&火炬会计公司(Mauersby & Storch Accounting)，纽约

对于大多数的人而言，会计工作就是数字整理和账目计算，通常认为那些就像在小路上漫步一样惬意。幸运的是，不是每一个人都那样看这份工作。例如，玛丽·哈里斯认为她的工作像高级会计师一样有趣，一部分原因是她是这家公司最专注的会计员工之一。

在这个特殊的星期一，玛丽到得很早，开始了漫长的一天里她的首要工作，并吃惊地发现她的电话响了。她接了电话，报上了她的名字。

“你好，我是彼得·谢帕德(Peter Sheppard)。这里是奥布斯特(Arbuclde)公司，我们为你的公司提供技术支持。我们在周末收到了几个这里的电脑有问题的投诉。我想我可以在早上所有人进来工作之前充当故障检修员。你的电脑有任何问题或者连接网络有任何问题吗？

她告诉他她还不知道。她打开了她的电脑，当电脑启动的时候，他解释了他要做的事情。

“我想在你的电脑上进行一些测试，”他说，“我能在我的屏幕上看见你键入的字，我想确认网络通顺。所以当你录入时，我想要你告诉我那是什么，然后我会检查这里是否是相同的文字或数字。好吗？”

梦魇一般的景象，她的电脑无法工作，失败的一天，不能完

成任何工作。她很高兴这个人能帮她。过了一会儿，她告诉他：“我到了登陆屏幕，我要输入我的ID。我现在键入它——M...A...R...Y...D。”

“到现在为止很好，”他说，“我看到了。现在，前进并输入你的密码但不要把它告诉我。不要把你的密码告诉任何人，甚至技术支持部门都不可以。我在这里只会看见星号——你的密码受到了保护所以我无法看到它。”这些都不是真的，但这对玛丽有意义。然后他说：“当你的电脑启动时告诉我。”

当她说它启动了时，他要她打开两个应用程序，然后她报告说他们运行得“很好”。

玛丽看到所有东西都运行正常，放心了。彼得说，“我很高兴可以确定你的电脑工作正常。听着，”他继续道，“我们刚才安装了一个更新程序，允许人们更改他们的密码，你可以给我几分钟时间让我能检查它是否工作正常吗？”

她对他的帮助很感激于是欣然答应了。彼得告诉她运行这个程序的步骤，允许用户修改密码，这是Windows2000操作系统的标准组件。“前进并输入你的密码，”他告诉她，“但是记住不要大声地说出来。”

当她完成这些时，彼得说：“只是为了这个快速测试，当它请求你的新密码时，输入‘test123’，然后在确认栏里再次输入它，点击确定。”

他告诉她从服务器断开的方法。他让她等待几分钟，然后再连接，这次试着用她的新密码登陆。它像有魔力一样工作着，彼得似乎很高兴，然后告诉她用初始密码改回去或者选择一个新的密码——再一次提醒她不要把密码大声地说出来。

“好了，玛丽，”彼得告诉她，“我们找不到任何错误，那很好。听着，如果有了任何问题，只要打电话到奥布斯特公司我们这里，我通常有特殊任务，但是这里的任何人都可以帮助你。”她感谢了他然后他们互相说了再见。

彼得的故事

彼得这个名字传播得很广——在他的学校里许多和他一起去学校的人听说他可以进行一些电脑风啸获得其他人不能获得的有用信息。当艾丽丝·康拉德找到他并寻求帮助时，他首先说的是不。为什么他要帮忙？当他第一次遇见她并试着和她约会时，她的拒绝让他倍受打击。

但是他拒绝帮忙似乎并没有让她吃惊。她说她认为一些事情他无论如何也办不到。那可能是个挑战，因为他当然确定他能办得到，那是他同意的理由。

艾丽丝拿出了一份关于一家交易公司的一些顾问工作的合

同，但是这份合同的条款似乎不是很好。在她回去请求获得更好的待遇以前，她想要知道其他顾问他们的合同条款都有些什么。

下面是彼得讲述这个故事。

当我知道它很容易时，我不想告诉艾丽丝任何事情，除了我可以做到人们认为我做不到的事情。好的，不容易，准确点，这次不容易，要做一系列的事情，但是还好。

我要给她展示这真实的一切，多潇洒。

星期一早上7：30之后一点点，我打电话给交易公司办公室并联系上了接待员，说我是这家公司处理他们退休金计划的人，想要和会计公司的人谈话。她有没有注意到会计公司的人还没有上班？她说："我想我几分钟之前见到过玛丽，我帮你联系她。"

当玛丽拿起电话时，我告诉她关于电脑故障的一些故事，那让她有些神经过敏，所以她很高兴的合作了。当我告诉她怎样修改她的密码时，我用同样的临时密码（我要她使用的：test123）快速登陆了系统。

进入并掌握了这里——我安装了一个小型程序允许我无论何时只要我想要就能访问这家公司的电脑系统，使用了一个我自己的秘密的密码。当我挂断玛丽的电话时，我的第一个步骤是清除登陆纪录，这样就没有人知道我曾经登陆过他（或她）的系统。这很容易。在我提升了我的系统权限之后，我下载了一个叫做clearlogs的免费的程序，我是在一个安全类的网站www.ntsecurity.nu找到它的。

到真正的工作时间了。我在所有文件里查找文件名带有"contract（译者注：合同）"关键字的文件，然后把它下载下来。我还在根目录里找到了更多——这些目录里包含了所有的顾问工资报告。所以我整理了所有的合同文件和一张工资清单。

艾丽丝可以细读这些合同看他们支付多少钱给其他顾问。让她辛苦地细读所有这些文件吧，我做到了她要我做的。

从我存放这些数据的磁盘里，我打印了一些文件当作证据给她看。我要她和我约会并请我吃午饭，当她翻阅这一堆纸时你可以看见她的表情。"没门，"她说，"决不。"

我没有拿出这些磁盘，它们是诱饵。我说过她不得不过来拿，希望也许她会对我的帮助表示感谢。

米特尼克信箱

这很令人惊讶，那些精心构造的请求可以轻易地让人们帮社会工程师做事。前提是引起基于心理作用的自动响应，这依赖于当他们觉得这个打电话的人是盟友时人们的心理捷径。

过程分析

彼得打给交易公司的电话表现的是社会工程学攻击的最基本的形式——一个简单的尝试，只需要一点点准备，首次尝试的工作，只用几分钟就能完成。

效果很好，玛丽，这个受害人，没有认为那是一些对她的欺骗或诡计，也没有提交报告或引起骚动。

彼得的计划使用了三种社会工程学策略。首先他让玛丽因为害怕而合作——让她认为她的电脑不能用了。然后他花时间让她打开了两个应用程序，这样她确定了她的电脑工作正常，让他们之间的好感增加了，感觉有了同盟一样。最终，他按照计划的一部分利用她的感激（他帮助她确认了她的电脑工作正常）让她进一步地合作。

通过告诉她在任何时候都不能说出她的密码，甚至不能告诉他，彼得彻底地完成了这一微妙的工作，让她觉得他是在关心她的公司文件的安全。这促进了她的信心，他肯定是合法的，因为他在保护她和她的公司。

警察的搜捕行动

想象一下这样一个情景：政府准备对一个叫做阿图若·森彻(Arturo Sanchez)的人展开行动，他在互联网上免费发布电影，好莱坞制片厂说他侵犯了他们的版权，他说他只是推动他们承认一个不可以避免的交易方式，所以他们开始做些事情让新电影可以免费下载。他指出（正确地）这是电影公司完全忽视的巨大的收入来源。

搜索证，谢谢

一天晚上回家迟了，他穿过街道查看了一下他家的窗户，即使他出去了也总是会留下一盏灯，但是现在，灯灭了。

他用力敲着邻居家的门直到他把人叫醒了，然后了解到确实有警察搜索了这座建筑。但是他们让邻居们待在楼下，所以他不能确定他们进入了哪个房间，他只知道他们离开时带走了一些很重的东西，可是他们把它掩盖了起来，他也说不出那些是什么，他们没有逮捕任何人。

阿图若检查了他的房间，坏消息是警察留下了一张纸条要求他马上打电话并在三天之内确定一次会面，更坏的消息是他的电脑不见了。

阿图若这天晚上消失了，他和一个朋友待在一起。但是一些不确定的东西困扰着他，警察知道了多少？他们最后会不会逮捕他，不给他任何逃走的机会？或者也不完全是这样，他可以解决这些事情而不用离开这里？

在你继续阅读之前，停下来思考几分钟：你能想象出任何途

径去找出警察知道你的哪些事情吗？傲慢的你没有任何政治上的联系或有朋友在警察局或者司法办公室，你可以想象任何途径，像一个普通公民一样，去获得这些信息吗？或者那只有一些有社会工程学技巧的人才能做到？

警察的故事

阿图若对他需要知道的这些很满意：首先，他拿到附近复印店的电话号码，打电话给他们请求使用他们的传真号码。然后他打电话给检察官办公室，找档案室。当他联系上档案办公室时，他介绍他自己是莱克镇的警官，说他需要和归档现行搜查证的办事员谈话。

“可以。”那位女士说。

“噢，好极了，”他回答，“因为我们昨晚搜捕了一个嫌疑犯，我想要了解宣誓书的位置。”

“我们用他们的地址归档。”她告诉他。

他说出了他的地址，她的声音几乎有些激动。“噢，是的，”她吐着泡沫，“我知道这个，‘版权侵犯’。”

“就是这个，”他说，“我在寻找宣誓书和许可证的副本。”

“哦，我这里正好有。”

“好极了，”他说，“听着，我现在在外面，有一个关于这件案子的秘密服务的十五分钟会议。我最近有点恍惚，把文件留在了家里，这里没有那些文件并且来不及回去拿了。我可以从你那里拿到副件吗？”

“当然，没问题。我把它复制一份，你可以到这里来拿它们。”

“好极了，”他说，“那真好。但是听着，我在镇子的另一边，你可以把它们传真给我吗？”

有了一个小麻烦，但是可以克服。“我们档案室没有传真机，”她说，“但是楼下的职员办公室有，他们可以让我用。”

他说：“我打电话到职员办公室问问看。”

职员办公室的女士说她乐意帮忙但是想要知道“谁来付钱？”，她需要知道账户代码。

“我拿到代码后再打电话给你。”他告诉她。

然后他打电话给DA办公室，再一次伪装成警官简单地询问了一下接线员，“DA办公室的账户代码是多少？”

没有丝毫犹豫，她告诉了他。

他打电话回职员办公室，提供了账户代码，原谅他进一步利用了这位女士：他要她上楼去拿那些副件来传真。

注意

使用那些对他的攻击有用的东西，比如电话和电脑，一个社会工程师如何知道那么多操作的详细资料（警察部门、司法办公室、电话公司和特殊的公司机构）？把它找出来就是他的生意，这些知识是一个社会工程师在交易中的库存，因为信息可以在他的行骗中帮助他。

掩盖足迹

阿图若还有其它组合的步骤去拿传真。总是有可能被人察觉到一些异样，他可能会在复印店发现几个侦探，他们随意地说着话，看上去很忙碌直到有人露面拿那个特殊的传真。他等待了一会儿，然后打电话回职员办公室确认那位女士已经发送了传真。到目前为止一切都很好。

他打电话给镇子对面的另一家连锁复印店，略施小计，“我对你的工作处理很满意，想写一封信给经理表示祝贺，她的名字是？”　有了这一基本信息，他又打电话给第一个复印店说他想和经理说话。当那个人拿起电话时，阿图若说：“你好，我是哈特菲尔德628店的爱德华(Edward)。我的经理安娜(Anna)要我打电话给你。我们有一个心烦意乱的顾客——有人把错误的复印店传真号码给了他，他在这里等一个重要的传真，可是他拿到的这个号码是你们复印店的。”这位经理答应马上叫一个人把这份传真发到哈特菲尔德的复印店。

当传真到了第二家复印店时阿图若早已经等在那里，他一把它拿到手，就打电话回职员办公室对那位女士表示感谢，还有“没必要把那些副件送回楼上了，你现在就可以把它们扔了。”然后他打电话给第一家复印店的经理，也告诉他把那些传真副件扔了。这样这里发生的事情就不会有任何纪录，只是有个人稍后回来问了些问题。社会工程师知道你决不会很细心的。

计划的这些方法，阿图若不需要支付第一家复印店收这些传真再把它发给第二家复印店的钱，并且如果露馅了警察先会找到第一家复印店，当他们安排去第二家复印店抓人时阿图若早已经拿到了他的传真。

故事的最后：宣誓书和许可证上显示警察已经有了阿图若盗版电影行为的充分证据。这就是他想要知道的。当天晚上，他穿过了州界线。阿图若开始了新的生活，在别的地方有了新的身份，准备再次开始他的活动。

过程分析

在任何检查官办公室工作的人，无论在哪里，总是免不了和执法部门的工作人员联系——回答问题、做好安排、获得讯息。任何足够勇敢的人都可以打电话声称自己是一名警官、代理州长

或者任何由他的语言来决定的角色。除非他很明显不了解术语，或者他有些神经紧张结结巴巴地结束他的话，或者用一些听上去不可信的方法，他可能甚至不会被问一个问题确定他的身份。那确实发生在这里，和两个不同的工作人员。

米特尼克信箱

问题的实质是没有人会对一个优秀社会工程师的欺骗免疫。因为普通生活的节奏，我们并不经常有时间深思熟虑再作出判断，虽然事实上那对我们很重要。复杂的情形，缺乏的时间，情绪的波动，或者精神的疲劳，都可以轻易地使我们分心。所以我们使用了心理捷径，没有经过谨慎和全面的分析就作出判断，一个像自动应答一样的心理作用。这些甚至适用于联邦、州和本地执法部门办公室。我们是所有人。

通过一个简单的电话就可以获得一个必需的支付代码，然后阿图若用一个故事打出了同情牌，“有一个关于这件案子的秘密服务的十五分钟会议，我有点心不在焉，把文件忘在了家里。”她自然对他这件事感到遗憾，然后偏离了她的职责去帮忙。

然后通过利用两个复印店，阿图若去拿那份传真时他让自己非常安全。进行传真时这里的一个变化让追踪足迹更加困难：代替把这些文件发给另一家复印店，攻击者可以给一个公开的传真号码，通过一个真实的地址在因特网上的免费服务将你收到的传真自动转发到你的邮箱地址里，他不会在任何地方露脸，没有人会认出他，邮箱地址和电子传真号码在完成任务后就可以扔了。

转换表格

一个我叫他迈克尔·帕克(Michael Parker)的年轻人，他是较晚完成better-paying论文的人之一，那通常是和大学学位挂钩的。他有一个机会参加一个本地大学的部分奖学金加教育贷款活动，但是那意味着要在晚上和周末工作才能支付他的租金、食物、汽油和汽车保险。迈克尔总是喜欢去找捷径，认为也许有另外的方法，一个只需要少量的努力就可以不用付钱的更快的方法。因为他从十岁第一次玩电脑时就开始学习计算机了，他着迷于发现它们是怎样工作的，他确信能更快看见自己的计算机科学学士学位，如果他可以“制造”它的话。

毕业生——没有荣誉

他可以入侵州立大学的计算机系统，找到成绩为B＋优秀或平均为A-毕业的人的档案，复制，然后加入他自己的名字，把它添加到当年毕业班的档案里。通过思考这些，不知道怎么了他有些

担心这个主意，然后他认识到肯定还有其它的在校生档案——学费支付档案，住房分配办公室，还有那些知道别的什么的人。仅仅建立课程和评分的档案会留下太多漏洞。

经过深入思考，他觉得这个方案只有在达到了他的目标时才能实现，学校里要有一个和他名字相同的毕业生，在任何适当范围的时间里获得过一个计算机科学学位。如果那样的话，他就可以在员工申请书里填写另一个迈克尔·帕克的社会保险号码，任何去大学核实姓名和社会保险号的公司都会被告知，是的，他有学位。（对大部分人而言不明显但是对他而言是显而易见的，他把一个社会保险号放在了工作申请里，然后如果被雇用了，就把他自己真实的号码填入新员工表格中。大部分公司都不会想去检查一个新员工在聘用时是否使用了一个不同的号码。）

登陆的麻烦

怎样在大学档案里找到一个迈克尔·帕克？他是这样着手的：

进入大学校园的主图书馆，他坐在一台电脑终端前，连入网络并访问大学的网站。然后他打电话给注册员办公室，当有人回应时，他运用了一个社会工程师耳熟能详的方法："我从电脑中心打电话来，我们正在更改一些网络配置，我们想要确定我们没有使你的访问中断。你连接的哪个服务器？"

"服务器？什么意思？"他问。

"当你查询学生档案信息时连接的哪一台电脑。"

回答是：admin.rnu.edu，储存学生档案的电脑名称。这是难题的一小部分：他现在知道了他的目标机器。

专业术语

哑终端：一台没有处理器的终端。只能响应简单的控制码和显示字符及数字。

他在电脑里输入了那个网址但是没有获得响应——和预期的一样，有防火墙阻止了访问。因此他运行了一个程序看看能不能连接上那台电脑的任何服务，然后发现了一个打开的端口运行着Telnet服务（允许一台电脑远程连接另一台电脑并像连接一台哑终端一样访问它）。获取访问权限所必需的是一个标准用户ID和密码。

他打了另一个电话给注册员办公室，这一次他仔细地倾听并确定在和另一个人说话。他遇到了一位女士，然后再次声称自己来自大学的电脑中心。他们安装了一个新的档案管理系统，仍处于测试阶段，想了解她是否可以正确访问学生档案。他给了她一个连接的IP地址并且告诉她怎样操作。

事实上，这个IP地址把她引到了学校图书馆迈克尔坐的电脑上。使用第八章中描述的相同步骤，他创建了一个登陆蜜罐--一个登陆界面的圈套--看上去就像是当她登录学生档案系统时通常看到的一样。"它没工作，"她告诉他，"它持续说'登陆不正确'。"

现在登陆蜜罐已经在迈克尔的终端上记录了她的用户名和密码。他告诉她："哦，这台机器里的一些账户仍然不能用，让我配置一下你的用户，然后再打电话给你。"小心的绑好未扣牢的一端，就像所有社会工程师精通的那样，他强调稍后再打电话，说测试系统还没有工作正常，如果她能使用它了，他们会打电话给她或者这里的其他人。

乐于助人的注册员

现在迈克尔知道了他要访问哪一个电脑系统，还有用户ID和密码。但是当他有了正确的名字和毕业时间时如何在文件里搜索这些信息？学生数据库是私有的，在学校建立它是为了对付大学特殊的需求和注册员办公室，并且有唯一的途径在数据库中访问信息。

首先清除这些最后的障碍：找到能把他带到神秘的搜索学生数据库中的人。他又打电话给注册员办公室，这一次成了另一个不同的人。他来自迪安工程办公室，他告诉那位女士，然后他问道："当我们访问学生档案出现问题时，我们该给谁打电话？"

几分钟以后他打电话给大学数据库管理员，上演了值得同情的一幕："我是注册员办公室的马克·塞乐。你能同情一下一个新人吗？很抱歉打电话给你但是这个下午他们都在开会，没有一个能帮助我的人在。我想要找回一份所有计算机科学学位的毕业生列表，从1990年到2000年的。他们今天就需要它，如果我没有它的话我这份工作就不会长久了。你会帮助一个处于不幸中的人吧？"帮助人们是这个数据库管理员要做的事的一部分，所以他特别耐心地告诉迈克尔一步一步的操作过程。

当他们挂断电话时，迈克尔已经把那几年全部的计算机科学毕业生的列表下载了下来。他搜索了几分钟，查找到了两个迈克尔·帕克，在他们中选择了一个，获得了这个人的社会保险号码和其它在数据库里的相关信息。

他就成了"迈克尔·帕克，B.S（译者注：Bachelor of Science 理科学士），计算机科学，光荣毕业，1998"。在这里，"B.S"是唯一恰当的。

过程分析

这次攻击使用了一个我之前没有谈到过的策略：攻击者请求机构的数据库管理员告诉他完成一个他不知道的电脑操作步骤。

一个强大并且有效的转换表格，相当于请求商店的所有者帮你搬运包含了消息的盒子，你只需要从他的架子上偷来放到你的车里就可以了。

米特尼克信箱

当电脑用户遇到社会工程学相关的威胁和攻击时，他们显得有些无能为力，那些技术存在于我们的世界中。他们有权使用信息，但是对什么是安全威胁缺乏详细了解。一个社会工程师会选定一名不懂得被寻求的信息有多么贵重的员工为目标，所以目标通常会答应陌生人的请求。

预防措施

同情、内疚和胁迫是社会工程师使用的三种非常流行的心理机制，这些故事证明了这些策略的有效。但是你和你的公司怎样才能消除这些攻击的威胁呢？

保护数据

这一章的一些故事强调了发送一份文件给你不认识的人有多么危险，即使当这个人是（或者表面上是）一名员工，这份文件是被发送到一个公司的电子邮件地址或传真机上。

需要制定非常详细的公司安全策略，保护贵重的数据不被发送给陌生人。需要制定严格的程序来传送有敏感信息的文件。当请求来自于陌生人时，必须有清晰的查证，要有依赖于敏感信息的不同的等级证明。

这里有一些可以考虑的方法：

建立知道需求（要求获得指定信息所有者的授权）。

保持一个处理这些事情的个人或者部门日志。

维护一张接受过特殊培训、被授权对外发送敏感信息的人员名单，要求只有这些人可以发送信息给工作组外部的人。

如果数据请求需要写入（电子邮件，传真，邮件），则要有另外的安全步骤检查这一请求是否真的来自这个人声称的地方。

关于密码

所有可以访问任何敏感信息的员工--在今天那事实上意味着每一位使用电脑的工作人员--都需要了解一些简单的操作，比如修改你的密码，即使是一小会儿都能导致一个严重的安全漏洞。

安全培训需要包含密码主题，关注什么时候和怎么样改变你的密码，什么是合法的密码，和将任何其他人卷入程序的危险性。培训尤其需要传达给所有员工的是他们应该怀疑任何涉及到他们密码的请求。

表面上看起来这是一条简单的传给员工们的信息，但不是，

因为这一观念的价值在于要求员工们了解像是修改一个密码这样简单的操作都能导致一个安全威胁。你可以告诉一个小孩 "穿过马路前注意两旁"，但是在这个小孩明白为什么那是重要的以前，你依赖于盲目的服从。要求盲目服从规则代表着忽视和忘记。

注意：

密码是社会工程学攻击关注的中心，那是我们致力于第16章的单独的部分，那里你可以找到详细的管理密码的推荐方针。

中心报告点

你的安全方针应该指定一个人或组为报告可疑行为（企图渗透你的机构）的中心点。所有员工都需要知道在任何时间打电话来试图电子或物理闯入的人都是可疑的，报告这些的电话号码应该始终放置在眼前，这样当员工们怀疑发生了攻击时就不需要去发掘它。

保护你的网络

员工们需要了解电脑服务器或者网络的名称不是无价值的信息，它能给一个攻击者基本的知识帮助他获取信任或者找到他期望的信息的位置。

特别的，像是数据库管理员之类的使用软件工作的人属于专业技术类别，他们需要在特殊的和非常限制性的规则下操作，验证打电话给他们请求信息的人的身份。

经常提供各种电脑帮助的人需要很好的培训识别哪些请求属于红色标记，暗示打电话的人可能试图进行社会工程学攻击。

这是有价值的笔记，可是来自这一章最后故事里的数据库管理员的观点，打电话的人是符合标准的：他是在校内打来的电话，并且他明显有站点登陆必需的用户名和密码。这正好再一次解释了的标准的身份验证（对任何请求信息的人）程序的重要性，尤其是像这个例子里打电话的人寻求帮助来获得机密档案的访问权限。

所有这些建议对于学院和综合大学要加倍考虑。电脑黑客行为是许多大学生喜爱的娱乐活动已经不是新闻了，也不要惊讶于学生档案--有时候是全体教员档案--是一个诱人的目标。这一陋习如此的泛滥，一些公司甚至考虑把大学加入敌对的外界环境，创建防火墙规则阻止以.edu结尾的教育机构地址访问。

我已经说清楚了，所有学生和职员的任何类型的档案都会是攻击的主要目标，应该得到很好的保护就像敏感信息一样。

训练技巧

大部分社会工程学攻击都可以轻易地被阻止，只要那个人知道自己掌握的是什么。

从公司的观点出发，有一些优秀培训的基本原则，但是同样需要另一些东西：多种途径提醒人们他们在学习什么。

使用屏幕溅射（splash screen，也叫程序启动画面的制作），当用户电脑启动时每天出现一个不同的安全消息。这条消息可以被设计为不能自动消失，要求用户点击这些消息确认他或她已经读过它了。

另一个我推荐的方法是启动一连串的安全提示。频繁的消息提示很重要，一个提示程序必须正在运行并且不能结束。在陈述的内容里，不应该在每一种情况里使用同样的措词。当他们变化措词或者使用不同的例子时，学习显示的这些消息更为有效。

一个卓越的方法是在公司的时事通讯上进行简短的宣传。这个主题不需要完整的专栏，虽然一个安全专栏的确有价值。另外，设计一个两或三栏宽的插入块，有点像是你们本地报纸的小型陈列广告。在每一次的时事通讯出版时，通过这个简短的注意力点呈现一个新的安全提示。

# 第九章 逆向骗局

圈套，在这本书的其它地方提到过（在我看来也许最好的电影永远是关于实施入侵的），迷人的叙说里安排了它巧妙的情节。在电影中圈套的一个准确的描述是顶级骗子运用的“金属丝”，这是提到的三种主要骗局之一的“重要的过程”。如果你想要知道一个专业的团队怎样只用一个晚上去实现一个骗局而迅速获得大量的金钱，这里没有更好的教材。

但是传统的入侵，他们的特殊花招都会依照一个模式。有时候一个诡计会被反向应用，这称为逆向骗局。这是一个迷人的手段，攻击者设定情况让受害人向他寻求帮助，或者一位同事正好发出了攻击者响应的请求。

这些是怎样实现的？你正打算发现它。

专业术语

逆向骗局：一种入侵手段，让被攻击者向攻击者寻求帮助。

友好的说服艺术

当一般人想象电脑黑客的样子时，通常会联想到阴暗的一面，一个孤独、内向、讨厌的人，他最好的朋友是一台除即时信息以外很难交流的电脑。社会工程师常常拥有黑客的技能，也有普通人的技能——在对立的光之尽头——通过你从未想过可能性的途径，使用得到良好发展的能力操纵人们谈论他们获取信息的方法。

安吉拉（Angela）的电话

地点：工业联邦银行，流域分行。

时间：上午11:27。

安吉拉维斯露斯基（Angela　Wisnowski）接到了一个电话，那个人说他刚刚得到了一大笔遗产，想要了解一些信息，关于不同类型的储蓄存款账户、存款单和任何她推荐的安全的可以正当获利的投资。她解释说有相当多的选择，问他是否可以过来坐下和她一起讨论它们。他说他一拿到钱就要去旅游，还有很多事情要安排。所以当她设法约束他的投资目标时，她开始推荐一些可能的类型，还给了他关于利率的详细资料，如果你很早地提现会发生什么，等等。

她似乎更进了一步，他说：“噢，对不起，我要接另一个电话。什么时候能和你继续这次交谈好让我作出一些决定？你什么时候出去吃午饭？”她告诉他是12:30，他说他会在那之前或者之后几天再打电话过来。

路易斯（Louis）的电话

银行总部使用每天都更改的安全密码，当分行的某个人需要从另一个分行处获得信息时，他可以通过证明自己知道这个每日密码来表明他有权访问信息。为了更深层次的安全性和机动性，一些银行总部每天都会发行多重密码。在一个被我称为工业联邦银行的西部海岸机构里，每一位员工每天都能收到一张有五个密码的列表，每天早晨在他或她的电脑上从A到E进行验证。

地点：相同。

时间：下午12:48，同一天。

路易斯霍普本（Louis Halpburn）对那个下午接到的电话不以为意，这个电话和一周里有规律的其它几次来电一样。

“你好，”打电话的人说，“我是尼尔韦伯斯特（Neil Webster），从波士顿3182分行打电话来。找安吉拉维斯露斯基，谢谢。”

“她在吃午饭，我能帮忙吗？”

“好的，她留了言请求我们传真一些关于我们的一个客户的资料给她。”

这个打电话的人听上去度过了糟糕的一天。

“通常处理这些请求的人请了病假，”他说，“我有一堆这些事情要做，已经在这里4个钟头了，我希望能在半个小时以后离开这里去和一个医生会面。

这样处理——给出了为什么其他人会觉得他很可怜的所有理由——这是使受害人软化的一部分。他继续说：“无论是谁接到了她的电话留言，传真号码已经不清楚了，大概是213什么的，其余的是什么？”

路易斯给出了传真号码，然后打电话的人说，“好的，谢谢，在我传真这些之前，我需要询问你密码B。”

“但是是你打电话给我的。”他说这句话时很冷淡，好让这个来自波士顿的人明白。

很好，打电话的人想。当人们在第一次温柔的推挤中没有跌倒时，很酷。如果没有少量的反抗，这份工作会太容易，我会变得懒散的。

他对路易斯说：“我这里的分行经理对我们发送任何东西之前的验证有些偏执，但是听着，如果你不需要我们传真这些信息，很好，不需要验证。”

“看，”路易斯说，“安吉拉会在大约半个小时后回来，我可以让她打电话给你。”

“我会告诉她今天我不能发送这些信息，因为你没有给我密码验证这些合法的请求。如果我明天没有请病假，我会再打电话给

她。”

“留言说‘紧急的’，别担心，没有验证我就无法操作，你可以告诉她我试着发送它但是你没有给我密码，好吗？”

在压力之下路易斯放弃了，从电话线的另一端传来一声烦恼的叹息。

“好的，”他说，“等一下，我要到我的电脑上去，你想要哪一个密码？”

“B。”打电话的人说。

他把电话放在桌子上然后很快又拿了起来。“3184。”

“那不是正确的密码。”

“它是正确的——B是3184。”

“我没有说B，我说的是E。”

“噢，该死的，等一会儿。”

另一次停顿，当他查看密码时。

“E是9697。”

“9697——正确，我在路上发送这份传真，好不好？”

“当然好，谢谢。”

沃尔特（Walter）的电话

“工业联邦银行，我是沃尔特。”

“嗨，沃尔特，我是影视城38分行的鲍勃格若博斯基（Bob Grabowski），”打电话的人说，“我需要你传真一份客户账户的签字样卡给我。”签字样卡上面有客户的签名，它也有验证信息，常见的例如社会保险号码、生日、母亲家族的姓氏，有时甚至是驾驶执照号码。这对于一个社会工程师来说唾手可得。

“确认信息，密码C是多少？”

“其他出纳员正在使用我的电脑，”打电话的人说，“但是我可以使用B和E，我记得它们。问我它们中的一个。”

“好吧，E是多少？”

“E是9697。”

几分钟以后，沃尔特依照请求传真了一份签字样卡。

堂娜普雷斯（Donna Plaice）的电话

“你好，我是安森莫（Anselmo）先生。”

“今天我能帮你些什么？”

“我想要了解保证金是否仍记入贷方，应该打哪个800号码？”

“你是这家银行的客户吗？”

“是的，我没有用过这个号码，现在我不知道我把它写在了哪里。”

“号码是800-555-8600。”

“好的，谢谢。”

文斯开普雷（Vince Capelli）的故事

斯伯克恩（Spokane）街巡警的儿子文斯很年轻的时候就知道他不会把生命花费在长时间的辛勤努力上，承受最低工资的风险。他人生的两个主要目标首先是离开斯伯克恩，然后是成就他自己的事业。朋友们的笑声一直伴随着他的大学生活，这只让他更加恼火——他们认为这很搞笑，他太失败了，想开创自己的事业却不知道从哪里开始。

文斯私下里其实知道他们是对的，他唯一擅长的事是在大学棒球队里当接球手，但是还不够好，拿不到大学奖学金，更别提职业棒球了。所以他能从哪里开始他的事业呢？

有一件事情在文斯的小组里的人一直没有弄明白：任何曾经是他们的东西——一把新的弹簧折刀，一对顶好的保暖手套，一个性感的女朋友，只要文斯喜欢，不久之后就会变成他的。他不需要偷窃或是鬼鬼祟祟地跟在任何人的后面，他不需要这样做。拥有它的人会自动放弃它，过后才会对这是怎样发生的感到惊讶。恰当的做法是请求文斯在任何地方都不要碰你的东西：他不了解他自己，人们似乎可以让他拿到任何他想要的东西。

文斯开普雷很年轻的时候就已经是一个社会工程师了，即使他从没听说过这个术语。

他的朋友们拿到了大学毕业证之后就再也没有笑他了。当其他人艰难地在城市周围寻找工作时（在那里你不会要说“你想要来点油炸食品吗？”），文斯的父亲送他去为一个年迈的巡警工作，这位巡警离开警局之后在旧金山开始了他自己的私人调查事业，他迅速发现了文斯的才能，并为他安排了一个适合的工作。

那是六年以前的事了。现在，坐着监视的无聊时间使他陷入痛苦，他痛恨从不诚实的配偶那里获取证据的部分，但是他感觉去搜集有用信息的任务是对自己的挑战，律师们想要了解一些可怜的穷人是否有足够的钱进行财产诉讼，这些任务给了他许多机会使用他的智慧。

像这一次他浏览了一个名叫乔马克欧兹（Joe Markowitz）的家伙的银行账户，乔可能暗地里处理了和他以前的一个朋友的交易，现在那位朋友想要知道如果他提出诉讼，马克欧兹有没有足够的家底让他拿回一些他的钱？

文斯的第一步是找出至少一个银行这一天的安全密码，但是两个会更好。这听上去像是几乎不可能的挑战：究竟是什么使得一个银行员工在他自己的安全系统里撞出一条裂缝来？问你自己——如果你想要这样做，你有任何主意去实现它吗？

对于像文斯这样的人来说，这太容易了。

如果你知道他们公司的行话和他们工作的内部术语，他们就会信任你。就像是把你当成了他们的内部成员一样，也像是一次秘密的握手。

我不需要太多这些工作的内部术语，不需要往头脑里灌输那些东西，开始工作只需要一个分行的电话号码。当我打电话到布法罗州比肯街办公室时，回应的人似乎是一个接线员。

“我是提姆艾克门（Tim Ackerman），”我说（任何名字都可以，他不会把它写下来），“这里的分行号码是多少？”

他知道这个电话号码或者分行号码，但是相当麻木，因为我只是要打这个电话号码（分行号码），不是吗？

“3182，”他说。就像这样，没有“你想要知道这个干什么？”或者任何问题，只因为它不是敏感信息，它被写在他们使用的每一张纸上。

第二步，打电话给一家银行的分行，我的目标在那里有存款。获取他们中一个人的名字，然后得到安吉拉外出午餐的时间，她12:30离开。到现在为止，非常好。

第三步，在安吉拉的午休时间打电话回同一家银行，说我从波士顿某某分行号码打电话来，安吉拉需要我传真这些信息，告诉我今天的密码。这是精彩的部分，出神入化。如果我要建立一个社会工程师测试，我会放上一些像这样的东西，你的目标起了疑心——为了一个好的理由——你仍然镇定自若直到打败了他，然后获得了你想要的信息。你不能通过背诵剧本里的句子或者学习日常事务做到这些，你要去了解你的目标，捕捉他的心情，像钓鱼一样控制他，放一点点线然后卷起，放线，卷起，直到你把他用网网起来，在船上用长板条拍打他！

我控制了他并且拿到了今天的密码，这是一个重要的步骤。对于大部分的银行，他们只使用一个密码，因此我可以在家里避开它。联邦工业银行使用五个，所以只使用五个中的一个的几率很小，有了五个中的两个，我就可以有更高的可能性完成这小小的戏剧的下一幕。我热爱“我没有说B，我说的是E”这一部分，当它生效时，实在是太漂亮了，并且它在大多数情况下都有效。

拿到三个可能会更好，事实上我想只用一个电话就拿到三个——“B”、“D”、“E”听上去很相似，你可以声称他们再次误解了你的意思，那样的话你肯定是在和一个真正弱小的敌人谈话。这个人不是，我拿到了两个。

每日密码是我拿到银行签字样卡的王牌。我打电话，然后那个人请求了一个密码，他想要C，我只有B和E，但这不是世界末日。在这一刻你必须保持镇定，听上去自信，保持正确的行为，真正的平滑。我使用一个技巧操纵了他：“有人使用了我的电脑，问我其它的这些。”

我们都是这家公司的职员，我们都在这里工作，让这个家伙方便些——这就是你希望受害人在那一刻心里想的。然后他按照剧本正确地操作了，选择了一个我提供的一个密码，我给出了正确的答案，他发送了签字样卡的传真。

打更多的电话我就可以知道客户使用的自动服务的800号码，差不多都有效，电子语音会把你请求的信息读出来。从签字样卡里我得到了目标所有的账户号码和他的PIN码（个人身份号码），因为那家银行使用社会保险号码前面的五个或者后面的四个阿拉伯数字。有了这些，我打电话给那个800号码，拨通号码几分钟后，我得到了这个家伙四个账户的最后余额，并且额外还知道了他最近的每一笔存款和取款操作。

每一件客户要求的事我都会给他们一些额外的特别的东西，好让他们高兴，毕竟，回头客才能让业务保持下去，不是吗？

过程分析

整个故事的关键是得到非常重要的每日密码，攻击者文斯使用了几个不同的技巧。

当路易斯不给他密码证明身份时，他开始用上了一点口头上的威胁。路易斯的怀疑是正确的——密码被设计成可以反向使用。他知道这些事情通常的流程，这个不知名的人将给他一个安全密码。这对文斯来说是决定性的时刻，成败在此一举了。

面对路易斯的怀疑，文斯简单地进行了控制，利用同情心（“去看医生”），压力（“我有一堆事要做，已经4个钟头了”），还有操纵（“告诉她你不肯给我密码”）。文斯很聪明，他事实上没有制造任何威胁，只是含蓄的表达了一个意思：如果你不给我安全密码，我就不会发送你的同事要的客户资料，并且我会告诉她我想要发送但是你不合作。

停，我们不能太草率地责备路易斯。毕竟，电话上的人知道（或者至少看起来知道）自己的同事安吉拉请求了一个传真。打电话的人知道安全密码，并且知道他们使用指定的字母来验证，还说他的分行经理有很严格的安全要求。似乎实在是没有任何理由不按他的要求进行验证。

并非只有路易斯，每一天都有银行职员在社会工程师面前放弃安全密码，难以置信却是真实的。

沙滩上有一根线，私人侦探的技巧介于合法与违法之间。当文斯获得分行的电话号码时他的行为是合法的，当他操纵路易斯告诉他两个每日安全密码时，他也是合法的，当他拿到一位银行客户的保密资料传真时，他越过了这根线。

但是对于文斯和他的老板来说，这是低风险的犯罪。当你偷钱或者商品时，会有人注意到它的发生。当你偷窃信息时，大多

数情况下没有人会发觉，因为他们仍然拥有这些信息。

米特尼克信箱

安全密码相当于提供了方便可靠的方法来保护数据，但是员工们需要了解社会工程师使用的骗局，并且要培训他们在任何时候都不要放弃使用密码。

被愚弄的警察

对于一个隐蔽的私人侦探或者社会工程师而言，当他轻而易举地拿到某个人的驾驶执照号码时，常常有很多机会——例如，你想要冒充另一个人来获得一些关于她的银行余额信息。

除非去偷那个人的皮包或是在恰当的时间透过她的肩膀窥视，找出驾驶执照号码应该是几乎不可能的事情，但是对于任何有适当的社会工程学技术的人而言，这几乎算不上挑战。一个特殊的社会工程师（我这样称呼他）——埃里克曼特尼（Eric Mantini）想要拿到驾驶执照和常规检查中的车辆登记号码。当埃里克需要那些信息的时候，他认为没必要冒风险去打DMV（机动车辆局）的电话然后反复使用同样的诡计。他想知道是否有什么途径可以简化处理。

也许这之前从没有人想过，但是他发现了一个瞬间就可以获得信息的方法，随时都可以。他利用了一个州机动车辆局提供的服务。许多州机动车辆局（或者你所在州这个部门的不同称呼）给了保险公司（当然还有私人侦探和其它组织）特权获取居民的这些信息，，州立法机关普遍认为把它授权共享有利于商业和社会的发展。

当然，DMV也对共享的数据类型进行限制，保险行业可以从文件里获得几种类型的信息，但是没有其它的。对私人侦探们（PIs）还有不同的限制，等等。

执法官员们通常有一个不同的惯例：DMV为任何宣誓过的治安官（如警察、警官、保安员等）提供档案里的任何信息，只要他能证明自己的身份。在埃里克所在的州，唯一需要的证明是一个DMV随同政府官员的驾驶执照号码一起发行的邀请码。DMV员工在共享信息之前始终验证匹配的官员名字，对照他的驾驶执照号码和其它部分信息——通常是生日。

社会工程师埃里克想要做的是通过一个执法官员的身份完全掩盖自己。他是怎样做到的呢？对警察使用逆向骗局！

埃里克的圈套

首先他打电话到电话号码咨询台询问州议会大厦DMV总部的电话号码，他被告知是503555-5000，当然，这个号码可以被普

通公众拨打。然后他打电话到一个附近的郡治安局并请求接通电传室——这是与其它执法机构通信的办公室，接收和发送国家犯罪数据库、本地许可证等等。当他联系上电传室时，他说他在找执法时使用的州DMV总部电话号码。

“你是？”电传室的警员问。

“我是奥，我要打到503-555-5753，”他说。这是骗局的一部分，一个无中生有的号码， DMV办公室和执法机构的电话使用同一个专用的区号，并且几乎可以确定后面的三个数字（前缀）也相同，他唯一需要知道的是最后的四个数字。

郡治安局电传室不会接到公众的电话，并且这个打电话的人已经有了这个号码的大多数，显然他是可靠的。

“是503-555-6127。”那位警员说。

那么现在埃里克已经拿到了这个执法官员打给DMV的号码，但是只有这一个号码并不能让他满意，应该还有更多的电话线路，埃里克需要知道那里有多少，并且需要知道每一个电话号码。

交换机

为了实现他的计划，他需要得到访问电话交换机（处理DMV的执法电话线路）的权限。他打电话到州电讯部门并声称自己来自Nortel——DMS-100（一种被广泛使用的电话交换机）的厂商。他说：“你能帮我转接到一个在DMS-100上工作的技术员吗？”

当他接通技术员时，他说自己是德克萨斯州的Nortel技术服务支持中心的工作人员，并解释说他们创建了一个管理员数据库来更新所有最近软件升级过的交换机。所有的一切都可以远程进行——无需任何交换机技术员参与，但是他们需要交换机的拨入号码，这样他们就可以直接从技术中心执行更新。

听上去完全是似是而非，但技术员还是把电话号码给了埃里克。他现在可以直接打电话到一个州电话交换机了。

为了防范外部入侵者，这种型号的商业交换机有密码保护，就像每一个公司电脑网络那样。任何使用后台电话盗用线路的优秀社会工程师都知道Nortel交换机为软件更新准备了一个默认的账户名：NTAS（Nortel Technical Assistance Support的缩写）。但是密码是什么呢？埃里克拨了几次，每一次都尝试一个常用的密码。输入和账户名相同的密码，NTAS，没有用，既不是“helper”也不是“patch”。

然后他试了一下“update”……登陆成功。典型的，使用一个常用的、容易被猜出的密码只比不用密码好一点点而已。

这有助于加快行动，埃里克或许已经足够了解那个交换机和

怎样像技术员一样规划和检修它。他曾经以合法的用户访问过交换机，现在他需要获得目标电话线路的完整控制权。他通过电脑在交换机上查询拿到的那个电话号码，执法人员打到DMV 的555-6127。他发现在同一个部门有19个其它的号码，显然他们要处理大量的来电。

交换机为每一个来电在20条线路中安排“搜寻”，直到找出一个空闲的线路。

他选择了一个排在第18位的线路号码，然后输入密码为那条线路增加呼叫转移。至于转接号码，他输入了他的新的、廉价的、预支付的大哥大，这种大哥大深受经销商的喜爱，因为它们足够便宜，可以在工作完成之后就扔掉。

现在激活了18线的转接，一旦办公室有17个电话占线，下一个来电就不会在DMV办公室响起，而是会转到埃里克的大哥大。他休息了一下并等待着。

一个打到DMV的电话

很快在那天早上8点之前大哥大就响了。这一部分是最好也是最美妙的，在这里埃里克，一个社会工程师，在和一个警察说话，而这个警察可以逮捕他或是拿搜索证指挥一次针对他的搜查。

并且打电话来的警察不是一个，在第一个之后，是一些。有一次，埃里克正坐在餐馆里和朋友们吃午饭，大约每五分钟就会接到一次电话，用一支借来的笔在餐巾纸上写下信息。他还是乐此不疲。

和警察说话丝毫不会打扰一个优秀的社会工程师，事实上，陶醉于欺骗这些执法机构或许增加了埃里克这个节目的乐趣。

按照埃里克的计划，通话的内容就像这样：

“DMV，我可以帮你吗？”

“我是安德鲁可欧探员。”

“你好，探员，今天我能帮你做些什么？”

“我需要驾驶执照号为005602789的Soundex。”他想要一张照片，这是执法人员熟知的术语——这很有用，比如，当警官们在外逮捕一名疑犯并想要知道他的样子时。

“当然，让我把记录调出来，”埃里克会说，“可欧探员，你属于哪个机构？”

“杰弗森郡。”然后埃里克会问这些热门问题：

“探员，你的邀请码是？你的驾驶执照号码是？你的生日是？”

打电话的人会给出他的私人验证信息。埃里克会用一些借口验证信息，然后告诉他验证信息已确认，并询问他想从DMV查找

的详细资料。埃里克会假装开始查找名称（打电话的人能听到键盘的敲击声），然后说一些比如“噢，该死，我的电脑又当机了。对不起，探员，我的电脑这个星期一直出毛病。你能再打回来让另一个办事员帮你吗？”

他结束通话的这种方法很保险，不会带来任何关于为什么他不能向警员提供帮助的猜疑。这时埃里克已经有了一个偷窃的身份——这些详细资料可以让他在任何时候拿到他需要的DMV秘密信息。

在收到几个小时的电话并拿到了许多邀请码之后，埃里克拨入了交换机并取消了呼叫转移。

几个月后，他开始为一些合法的PI（私家侦探）公司工作，他们不想知道他是怎样获得信息的。当他需要时，他会再次拨入交换机并开启呼叫转移，然后收集另一些警员证件。

过程分析

让我们来回顾一下埃里克一连串的欺骗工作。在第一个成功的步骤中，电传室把DMV的密码号码给了一个完全陌生的人，而没有进行任何验证。

然后州电讯局的某个人做了同样的事，把埃里克当成了硬件厂商的工作人员，并且把拨入DMV电话交换服务的电话号码给这个陌生人。

埃里克可以进入交换机很大程度上是因为交换机厂商脆弱的安全习惯,他们的交换机都使用同样的帐户名。社会工程师可以轻易地猜到密码，毫无疑问，交换机技术员会像大多数人一样选择易记的密码。

有了交换机的访问权限，他把执法人员使用的一条DMV电话线路设置呼叫转移到了他的大哥大上。

然后，在这个骗局的高潮部分，他操纵了一个又一个的执法官员，不仅得到了他们的邀请码，还得到了他们的私人验证信息，这样埃里克就可以假扮他们。

当然还必须要有足够的技术知识来完成这个绝技，少了这些人们就会知道他们在和一个冒名顶替的人谈话。

这个故事中的另一个现象是为什么人们不问“为什么？”，为什么电传室办事员要把这些信息给一个他不知道的郡代理（或者，也可以说，一个自称是郡代理的人）而不是建议他从他的代理同事或上司那里获得这些信息？我可以提供的唯一答案是人们很少问这个问题。他们没有想到去问？还是他们不想听上去不友好？也许，任何更多的解释都只是无用功，但社会工程师不关心为什么，他们只关心这一事实可以让获取信息变得容易，否则这将成为挑战。

米特尼克信箱

如果你的公司有电话交换机，管理它的人在接到硬件商的电话并被请求告知拨入号码时会怎样做？顺便问一下，那个人曾经更改过交换机的默认密码吗？那个密码是不是一个在任何字典里都可以找到的可以轻易猜出的密码？

预防措施

使用恰当的安全密码可以构建了一个有效的保护层，而使用不恰当的安全密码则比不用安全密码更糟糕，因为它带来了并不真正存在的安全幻想。有很好的密码但你的员工是否使用它们？秘密？

有口头安全密码的任何公司都必须清楚地向员工说明什么时候和怎么样使用这个密码。有了适当的培训，这一章第一个故事中的人物就不会依赖于他的本能，在询问一个陌生人安全密码时被轻易突破。他感觉这种情况下不应该询问密码E，但是缺乏一个清晰的安全策略--和优秀的判断能力--他轻易地让步了。

当员工遇到不恰当的安全密码请求时安全程序应该要有应对的步骤。应该培训所有的员工直接报告任何可疑情况和验证信息（例如一个每日密码）请求，当核查请求者身份失败时也应该报告。

至少，员工应该记录呼叫者的名字、电话号码、办公室或部门，然后再挂断。在回电之前他应该检查那个机构是否真的有这个员工，打回的电话号码是否与在线公司目录上的电话号码匹配。大部分时间都可以使用这个简单的策略核实呼叫者的身份。

当公司用一个发行的电话目录代替一个在线版本时，身份核实要更加严谨。人员雇用，人员离开，人员调动，工作位置，工作电话，这些黄页在发行之后的第二天就应该废弃不用，因为社会工程师知道怎样修改它们。如果员工无法从一个独立来源核实电话号码，她应该被指定通过另外一些方式核实，例如联系员工经理。

第三部分入侵警报

第十章 进入内部

为什么一个外部人员伪装成一个公司员工会这样容易？为什么他们的扮演会如此有说服力甚至有高度安全意识的人都会受骗？为什么欺骗十分了解安全程序的人会这样容易？

在你阅读这一章的故事时思考这些问题。

警卫的麻烦

日期/时间：10月17日，星期二，凌晨2:16

地点：Skywatcher航空公司位于图森（Tucson，美国亚利桑那州南部城市）市郊的制造车间。

警卫的故事

在这个袅无人烟的制造车间走廊上，听着脚后跟反复敲打地板的声音，勒罗伊格林（Leroy Greene）觉得这比整个晚上都守在警卫室的视频监控器前要好多了，在那里除了盯着屏幕之外他不能做任何事情，不能看杂志或者他的带皮边的圣经。你只能坐在那里看着显示屏上一动不动的画面。

但是在走廊里走动他至少还可以活动一下腿脚，并且还可以在走动时甩一下胳膊和肩膀，这也让他有了一点点锻炼。虽然这对于一个在全城高中冠军橄榄球队打右内边锋的人来说算不上真正的锻炼，但是他想，工作就是工作。

他转向了东南角并开始沿着走廊俯视半英里长的生产场地，然后他发现有两个人越过了直升飞机制造部分的边线，站在那里似乎在互相指点着什么。在晚上这个时候看见的陌生人，“最好检查一下，”他想。

勒罗伊从通往生产场地的楼梯一直走到那两个人后面，他们没有察觉到他的接近，直到他在旁边走了好几步。他说：“你们好，我能看看你们的安全证件吗？谢谢。”勒罗伊想使自己的语气在这个时候尽量温和些，他知道过于强硬会变得像是在威胁。

“你好，勒罗伊，”他们中的一个把他的证件上的名字读了出来，“我是汤姆斯第尔顿(Tom Stilton),来自菲尼克斯的公司营销办公室，我在城里开会，想向我的朋友展示一下世界上最好的直升飞机是怎样制造的。”

“好的，先生，你们的证件，谢谢。” 勒罗伊说，他不禁觉得他们似乎太年轻了，那个营销员看上去才刚刚读完中学，另一个人长发披肩，看上去大概十五左右。

理过发的人想从口袋里拿出他的证件，等他把所有的口袋都找过一遍之后，勒罗伊开始觉得有些不妙，“该死，”那个人说，“一定是放在车上了，我这就去拿——只要10分钟，我去一趟

停车场就回来。”

勒罗伊有自己的打算，“先生，你说你的名字是？”他问道。勒罗伊谨慎地写下了回答，然后要求他们和他一起去警卫室。在到第三个走廊的升降梯上，汤姆聊到他在公司才6个月，并希望自己没有惹任何麻烦。

安全监控室里，其他两个值夜班的警卫和勒罗伊一起盘问了那两个人。斯第尔顿给出了他的电话号码，并说他的上司是朱迪安德伍德（Judy Underwood），然后给出了她的电话号码，这些信息都在电脑上得到了确认。勒罗伊把其他两个警卫拉到一旁讨论该怎么做，没人想把这件事情弄错，于是三个人一致认为他们最好打电话给那个人的上司，即使那意味着要在半夜把她叫醒。

勒罗伊亲自打给了安德伍德女士，解释了他是谁并询问她有没有一个叫汤姆斯第尔顿的雇员。

她听上去似乎还是半睡半醒，“是的。”她说。

“好的，我们2：30的时候在生产线上发现了他，他没有身份证件。”

安德伍德女士说：“让我和他谈话。”

斯第尔顿拿起电话，说：“朱迪，真的很抱歉这些人在半夜把你叫醒，希望你不要责怪我。”

他一边听一边说：“为了新的新闻稿会议，明天上午我无论如何都要在这里。不管怎么样，你收到关于汤普森生意的电子邮件了吗？我们需要在星期一早晨和吉姆见面所以我们不能没有这个。我还要在星期二和你一起吃午餐，对吗？”

他倾听了一会儿，说了声再见并挂上了电话。

这让勒罗伊始料不及，他本来想要拿回电话让那位女士告诉他一切正常的。他想他也许应该再打电话给她，但还是改变了主意，他已经在半夜打扰了她一次，如果他再打过去，她可能会生气并向他的上司投诉。“何必自找麻烦呢？”他想。

“我是不是可以向我的朋友展示剩下的生产线了？” 斯第尔顿问勒罗伊，“你想要跟着我们吗？”

“继续吧，”勒罗伊说，“四处看看。只是下次可不要忘了带上证件，如果你想要去设备车间的话，先让警卫知道——这是规定。”

“我会记住的，勒罗伊。”斯第尔顿说，然后他们离开了。

不到十分钟，警卫室的电话响了，是安德伍德女士，她想要知道“那个家伙是谁？！”。她说她试着问一些问题，但他一直在谈论和她一起吃午餐的事，她根本不知道他到底是谁。

警卫室的人打电话让前厅和大门的警卫到停车场去，得到的回应是那两个年轻人在几分钟前离开了。

说了这个故事之后，勒罗伊总是要这样结尾说：“老天爷，我

的上司就差没吃了我，还好没丢了工作。”

乔哈珀（Joe Harper）的故事

来看看他能完成哪些事，17岁的乔哈珀已经有超过一年的非法潜入建筑物历史了，有时候是白天，有时候则是晚上。音乐家和鸡尾酒服务生晚上都要上班，作为他们的儿子，乔有太多自由时间了。他的故事讲述了这件事情是怎样发生的，很有启发性。

我的朋友肯尼想要当一名直升机飞行员，他问我能不能带他到Skywatcher工厂去看制造直升机的生产线，他知道我以前到过一些其它地方。一股肾上腺素冲动使你很想看看能不能溜进禁止进入的地方。

但是你不能大摇大摆的走进一个工厂或办公楼，必须考虑周全，做很多计划，对目标进行完整的侦查。查看公司的网页名称和标题、报告结构和电话号码，阅读剪报资料和杂志文章，精确的调查是我谨慎的标志，所以我能运用和员工一样多的信息应对任何盘问我的人。

那么从哪里开始呢？首先我在互联网上查找这家公司的位置，了解到公司的总部在菲尼克斯，好极了。然后我打电话过去请求接通营销部门：每家公司都有一个营销部门。一位女士接了电话，我说我属于蓝铅笔绘图公司，我们想知道是否有人对我们的服务感兴趣和我们应该找谁。她说应该找汤姆斯第尔顿，我询问他的电话号码，她说他们不能透漏这些信息，但是可以对我破例。电话里响起了语音提示，他的留言说：“我是负责绘图工具的汤姆斯第尔顿，分机3147，请留言。”当然——他们不会公布分机号，但是这个人把它放到了他的语音信箱里。非常好，现在我有了一个名字和分机号。

另一个电话，打给同一个办公室。“你好，我在找斯第尔顿，他不在，我想问他的上司一些简单的问题。”那位上司也出去了，但是当挂上电话的时候，我知道了她的名字，并且她也恰好把分机号留在了她的语音信箱里。

我也许可以不费吹灰之力地骗过大厅的警卫，但是我查看过那个工厂，我想我记得在停车场周围有一个围墙，这意味着会有一个警卫在那里检查进入的车辆。在晚上他们也可能会记录车牌号码，所以我不得不在跳蚤市场买了一个旧的车牌。

但是首先我必须拿到门卫室的电话号码。我等了一会儿，这样如果碰到同一个接线员的话她就不会认出我的声音，然后打过去说：“我接到投诉，Ridge路门卫室的电话有些断断续续的问题——现在还是那样吗？”她说她不知道但是可以为我转接。

“Ridge路警卫室，我是赖安。”那个接电话的人说。我说，“你好，赖安，我是本。你这里的电话有问题吗？”他只是一

个低层的警卫但我猜想他大概受过一些训练，因为他马上说，“本什么——你的姓是？”我像是没听到他的话一样继续说，“之前有人说有问题。”

我可以听到他放下电话大声说，“嘿，布鲁斯，罗杰，这个电话有问题。”然后他说，“不，我不知道有问题。”

“你们那里有几条电话线路？”

他已经忘了问我的名字。“两条。”他说。

“现在的这个是？”

“3140。”

到手了！“它们都工作正常吗？”

“好像是的。”

“好的，”我说，“听着，汤姆，如果你的电话有任何问题，可以在任何时间打电话到电信来找我们，我们会帮忙的。”

我和我的伙伴决定第二天晚上去参观工厂，下午晚些时候我打到警卫室，用那个营销员的名字说，“你好，我是负责绘图工具的汤姆斯第尔顿，我们已经接近了最后期限，所以我叫了几个人到这里来帮忙，有一两个可能要到晚上才来，到时候你还在吗？”

他很高兴能这样说，不，晚上他不在。

我说，“好吧，留个信给轮班的人，好吗？看到两个找汤姆斯第尔顿的人，就挥挥手让他们进来——好吗？”

好的，他说，没问题。他写下了我的名字、部门和分机号，并说他会办好的。

凌晨两点之后我们开车到了大门口，我说出了汤姆斯第尔顿的名字，然后一个昏昏欲睡的门卫就告诉了我们进去的通道和停车地点。

当我们走进工厂时，大厅里还有另一个警卫在那里进行常规的临时签到登记。我告诉这个警卫说我有一个报告需要在早上准备好，我这位朋友想要看看车间。“他对直升机很着迷，”我说，“他大概想学怎样驾驶。”他要我的证件，我把手伸进口袋，四处找了一下，然后说我肯定是把它忘在车里了，我这就去拿。我说，“大概十分钟。”他说，“没关系，好吧，签到就是了。”

从生产线一路走下来走下来——没遇到任何阻碍，直到一个叫勒罗伊的树干挡住了我们。

在警卫室里，我没有表现出不安和受惊，当事情不妙时，我就开始说些像是我真的很激动的话，比如我真的是那个人，他们不相信我让我很生气。

他们开始讨论或许他们应该打电话给那位我说是我上司的女士，然后从电脑上查到她家里的电话，我站在那里想，“一有机会就逃跑。”但是这里有停车场大门——即使我离开了这里，他们只要把大门关上我们就出不去了。

当勒罗伊打电话给那位斯蒂尔顿的上司并把电话递给我时，那位女士向我大叫“是谁，你是谁！”，我只是继续说着，就像我们在进行一次愉快的对话，然后挂断。

要多长时间才能想起某个能在半夜给你一个公司电话号码的人？我认为我们有至少15分钟的时间在那位女士打电话到警卫室往他们的耳朵里塞臭虫之前离开这里。

我们以最快的速度离开了这里，但没有看上去很匆忙，当看到大门的守卫挥手让我们过去时，真的很高兴。

过程分析

值得注意的是这个故事基于一个真实的事件，入侵者的确是青少年。这次入侵是闹着玩的，他们只是想看看能不能做到，但是如果这对两个青少年而言很容易，那对于成年的小偷、商业间谍或恐怖分子就应该更容易。

三个有经验的警卫怎么会允许两个入侵者就这样离开的呢？而且是任何明眼人都会觉得非常可疑的青少年？

勒罗伊起先的怀疑是正确，他很恰当地把他们带到了警卫室，然后盘问这个自称为汤姆斯第尔顿的家伙，核对他给出的姓名和电话号码，也很恰当地打了电话给那位主管。

但最后他还是被这个年轻人装出来的自信和愤慨给骗了，他认为这不像是一个小偷或入侵者的行为——只有真正的员工才会这样做，他大概是真的。勒罗伊应该训练使用可靠的验证方式，而不是凭感觉。

当这个年轻人把电话挂上而不是还回来让勒罗伊直接从朱迪安德伍德那里确认他有理由这么晚了还在工厂时，为什么他没有更多的怀疑？

勒罗伊被一个很明显的花招给骗了，但是当时从他的角度来看：一个中学毕业的人，关系到工作，不能确定是不是应该在半夜再次打扰一位公司主管。如果你是他，你会再打过去吗？

当然，再打一个电话过去并不是唯一的选择，警卫们可以怎么做呢？

在打电话之前，他可以要求他们两个人拿出照片证明：他们是开车到工厂的，所以至少会有一个人有驾驶执照，那么他们最初使用的假名字就会马上暴露（一个专业人员会预备好伪造的ID，但是这两个青少年没有这样做）。无论如何，勒罗伊都应该检查他们的身份证件并写下这些信息。如果他们都坚持说证件不在身上，勒罗伊就应该和他们一起去拿“汤姆斯第尔顿”声称放在车上的公司ID证件。

米特尼克信箱

社会工程师通常有很有魄力，他们反应迅速并且表达能力相当强，也很熟练转换人们的思考过程使其合作，任何一个认为自己对这种控制免疫的人都低估了这种能力和社会工程师的破坏力。

一个优秀的社会工程师，另一方面，绝不会低估他的对手。

在打完电话以后，应该要有一个警卫陪着那两个人直到他们离开工厂，然后送他们到他们的车里并写下车牌号码。如果他的观察力足够敏锐，就会注意到车牌（攻击者从跳蚤市场买来的）的注册号无效——这样就有了足够的理由把他们留下来进行更多的调查。

垃圾搜寻

垃圾搜寻是指从目标的垃圾中搜寻有用的信息，你可以了解到的目标信息数量十分惊人。大部分人不会仔细去想他们在家里都扔了些什么：电话清单、信用卡声明、医疗处方瓶子、银行结单、和工作有关的材料等等等等。

在工作中，员工们必须知道从垃圾中翻找出的信息也许对他们而言是有用的。

在我的中学时代，我常常跑到本地的电话公司大楼后面翻寻垃圾——大部分时间是一个人，偶尔也会和对电话公司感兴趣的朋友一起。当你成为一个垃圾搜寻老手之后，你会学到一些诀窍，比如怎样努力避开公共厕所的袋子，必要的耐磨手套等。

垃圾搜寻并不有趣，但很有成效——公司内部电话目录、电脑手册、员工列表、怎样设定交换机的废弃资料、等等——在这里都能获得。

我计划在新手册发行的当天晚上进行搜寻，因为垃圾箱里会有很多被轻率扔掉的旧手册。在其它不固定的时间，我也去搜寻备忘录、信件、报告等，它们会提供一些珍贵而有趣的信息。

到了以后我就找一些纸箱，把它们拿出来放在一边，如果有人问我（偶尔会发生）我就说一位朋友要走了，我找些箱子帮他整理。警卫从未发觉所有的文件都被我放进箱子带回家了，有时候他叫我离开，我就到另一个电话公司中心办公室去。

术语

垃圾搜寻：从一家公司的垃圾中（通常是在外部和易受攻击的地方）找出被抛弃的可用于社会工程学攻击的信息，例如内部的电话号码或资料。

我不知道现在怎么样，但是在过去可以轻易地知道哪一个袋

子里会有有用的东西，地面清洁和自助餐厅的垃圾放在巨大的袋子里，当办公室的废纸篓全部摆满一次性的白色垃圾袋时，清洁人员就一个一个地把它们拿出来捆好。

有一次，当我和一些朋友一起搜寻时，我们弄到了一些被撕碎了的纸片：有人还特意撕得很小，全部都扔进了五加仑的专用垃圾袋。我们拿着袋子到了一家本地的油炸圈饼店，把这些碎片全部倒在一张桌子上，然后开始把它们一个个地拼起来。

我们全都是问题实干家，这个巨型智力拼图很有挑战性——但能得到比小孩子更多的酬劳。完成的时候，我们一起拼出了这家公司某个关键计算机系统的全部用户名和密码列表。

垃圾搜寻值得我们去冒险和努力吗？当然值得，甚至比你想的要好，因为风险为零。这在当时是真的并且在今天也是：只要你没有犯罪，翻寻别人的垃圾是百分之百合法的。

当然，电话盗打者和黑客们并不是唯一瞄准垃圾桶的人，这个国家的警察局经常翻查垃圾，很多小型贪污案的幕后主使就是因为这些从他们的垃圾中提取的证据被判了刑。情报机构，包括我们自己，采用这种方法已经有几年了。

可能这对于詹姆士邦德而言太卑鄙了——电影人更愿意看到他用计谋去打败坏人，而不是在垃圾堆中努力奋斗。当一些有价值的东西周围堆放着香蕉皮、咖啡渣、报纸和食品目录时，现实中的特工很少有放弃的，特别是如果搜集这些信息不会给他们带来危险的话。

现金买垃圾

大公司也玩垃圾搜寻的游戏。报社在2000年6月忙了好一阵子来报道甲骨文公司（这家公司的CEO拉里埃里森恐怕是这个国家最坦率地反对微软的人了）雇用的一家侦探公司被逮了个正着的事，那些侦探想要弄到竞争性科技协会（ACT，译者注：这个协会是微软为应对反托拉斯案创立的）的垃圾，但是不想有被抓住的风险。据新闻报道，他们派的那位女士想用60美元现金向一位看门人买下ACT的那些垃圾，结果被拒绝了，她第二天晚上再回来的时候，把价钱上升到给清洁工500美元和给主管200美元，但那位清洁工拒绝了这笔意外之财并且汇报了这一情况。

领先一步的在线新闻记者迪克兰迈古拉引用了很多资料，他在连线新闻故事中使用的标题是“甲骨文紧盯微软”，《时代》周刊紧跟甲骨文的埃里森，他们报道的标题是“偷窥的拉里”。

过程分析

基于我自己的经历和甲骨文的经历，你可能会感到奇怪：为什么人们要惹麻烦去冒险偷别人的垃圾？

答案，我认为，是因为风险为零并且好处多多。好吧，也许去贿赂看门人增加了成功的几率，但是在任何愿意变脏一点的人看来，完全没有必要去贿赂。

对于一个社会工程师而言，垃圾搜寻自有它的好处，他可以得到足够的信息来指引他对目标公司的攻击,这些信息包括备忘录、会议议程、信件和那些泄漏的姓名、部门、标题、电话号码与工程任务。垃圾桶里出产公司机构图、法人结构信息、旅行时间表等等，这些资料对内部人员而言价值不高，但是它们在攻击者看来可能是很贵重的信息。

马克约瑟夫爱德华兹（Mark Joseph Edwards）在他的书《Windows NT因特网安全》中谈到“整份报告因为排版错误而被扔了，密码被写在残余的纸片上，‘当你离开的时候’的讯息上有电话号码，所有文件的文件夹还在里面，磁盘和录音带没有被清除或销毁，这些都可以帮助一名想要入侵的人。”

作者接下来问道：“你的清洁队里都有些什么人？你不允许清洁工进入计算机机房，但是别忘了那些垃圾桶。如果联邦机构认为有必要对那些有权使用他们的废纸篓和碎纸机的人进行后台检查，你或许就更应该这样做。”

米特尼克信箱

你的垃圾可能是你对手的财富。我们对那些在我们的个人生活中扔掉的东西考虑得并不多，有什么理由让我们相信人们在工作中会有不同的态度呢？这些都涉及到训练员工了解威胁（搜寻有用信息的坏人）和弱点（没有被粉碎或完全清除的敏感信息）。

被羞辱的上司

当哈伦福尔蒂在星期一早晨像往常一样到郡公路局上班，并说他从家里出来得太急忘了带证件时，没有人对这件事有任何想法。那个警卫在这里工作了两年，天天看着哈伦进进出出，她给了他一个临时员工证件并要他签上名。然后他继续行动。

两天以后，灾难降临了。那个故事在整个公路局里快速传播着，有一半的人不敢相信这是真的，其余的人则不知道是哈哈大笑好还是该同情这个可怜的人。

毕竟，乔治阿达姆松（George Adamson）是个友好而富于同情心的人，是他们曾经有过的最好的上司，这些不应该发生在他身上。当然，如果这个故事是真的的话。

星期五晚些时候，当乔治把哈伦叫到办公室里并尽可能温和

地告诉他，星期一他要到卫生局的新工作上报到时，麻烦开始了。对于哈伦而言，这比被解雇更坏，他绝不能忍受这种羞辱。

那天傍晚他独自一人坐在阳台上注视着来来往往的车辆，最后他发现那个被人称作“战争游戏男孩”的大卫正骑着电动车从学校回来。他把大卫叫住，给了他一瓶特意买来的红色密码（译者注：百事可乐的一种桃红色威士忌），然后提出了一个交易：用最新的电视游戏机和六个游戏换取少量的电脑帮助和一个保守秘密的承诺。

在哈伦解释了任务之后——没有任何危险的细节——大卫同意了，他详细描述了哈伦要做的事情，买一个调制调解器，进入办公室，找到一台旁边有多余电话插口的电脑，插上调制调解器，把它放到桌子下面一个没人能看见的地方。接下来的事情有一定的危险，哈伦要坐在那台电脑上安装一个远程控制软件包并运行，在这个办公室里工作的人可能会在任何时间出现，或者某个经过这里的人会看见他在别人的办公室里。哈伦非常紧张，因为他很难读懂大卫为他写下的使用说明，但他还是办到了，并且在没有任何人注意到的情况下溜了出来。

埋下炸弹

大卫吃完晚饭后留了下来，两个人坐在哈伦的电脑面前，这个男孩花了点时间拨入那个调制调解器，获得访问权限，然后到达了乔治阿达姆松的机器。这并不很难，乔治从没有过任何防范措施（比如更改密码），并且总是让这个或那个人为他下载或Email某个文件，这样一来，办公室里的每个人都知道了他的密码。稍微搜索之后大卫找到了一个名为BudgetSlides2002.ppt的文件，他把它下载到了哈伦的电脑上，然后哈伦让他先回家，几个小时候再来。

当大卫回来的时候，哈伦要他再次连接到公路局的电脑系统并用一个相同的文件覆盖掉之前找到的那个文件。之后哈伦给大卫看了那个电视游戏机，并许诺一切顺利的话，第二天他就可以拿到它。

吃惊的乔治

想不到预算听证会这种很无聊的事情能让这么多人感兴趣，郡参议会的办公室里挤满了记者、专业兴趣组的代表、公众成员，甚至还有两个电视新闻组。

乔治在这些会议上总是有些战战兢兢。郡参议会掌管着财政，如果他不能拿出一份有说服力的报告的话，公路局的预算就会被否决掉，然后每个人都会开始抱怨道路上的洞坑、不亮的红绿灯和危险的十字路口，并且责怪他，接下来整整一年的生活都

会变得极度拮据。但是这天晚上当他被介绍时，他很有自信地站了起来。他已经为这个报告工作了六个星期，还给他的妻子、高层的同事和一些敬重的朋友试验过这个PowerPoint演示，每个人都认为这是他有过的最好的报告。

起先的三个PowerPoint图片显示得很好，换了个心情，每一个参议会的成员都专心起来，他有效地表达了自己的观点。

然后一切都突然变得不正常了，第四张图片应该是去年新扩建的公路日落时的美丽画面，却变成了一些令人难堪的东西，一张来自《阁楼》或《好色客》杂志的图片。当他匆忙点击便携式电脑的按钮进入下一张图片时，他听到下面的观众全都倒吸了一口气。

这一个更糟，简直就难以想象。

他仍然试图单击到另一张图片，但观众里的某个人拔下了放映机的插头，然后主席重重地敲下了他的槌子，压过喧闹大声宣布会议暂停。

过程分析

利用一个少年黑客的专业技术，一个不满的员工进入了他的部门主管的电脑，下载了一个重要的PowerPoint文件，并把一些幻灯片替换成了几张令人难堪的图片，然后把这个文件放回到那个人的电脑。

通过一个插好的调制调解器，这个年轻的黑客可以从外部拨入并连接到办公室的某台电脑。这个男孩预先安装了一个远程控制软件，只要连接到那台电脑，他就可以访问系统里的每一个文件。之前这台电脑已经被连接到了网络，他也知道了这个主管的用户名和密码，他可以轻易地访问主管的文件。

包括搜索杂志图片的时间，总共才用了几个小时，结果让一个好人的声誉受到了难以估量的损失。

米特尼克信箱

大多数被调动、解雇或被降职的员工都不是麻烦，但只要有一个就可以让公司认识到所有的防范措施都太迟了。经验和统计图表都清晰地表明了企业面临的最大威胁来自于内部人员，内部人员知道哪里有贵重信息，攻击哪里可以造成最大伤害。

营销员

一个舒适的秋天上午，彼得米尔顿（Peter Milton）走进了光荣汽车零配件（一个汽车零件市场的本土零件批发商）丹佛区域办公室大厅，他在接待处等待着，那个年轻的女士正在登记一个访客，给一个打来电话的人驾驶指引，应付接连不断的人，所有

这些差不多都是在同一时间。

“你是怎样学会同时处理这么多事情的？”彼得在她有空接待他的时候说，她笑了，显然很高兴。他来自达拉斯办公室的营销部，他告诉她，并说亚特兰大销售区预的迈克塔尔伯特（Mike Talbott）要和他会谈。“今天下午我们要一起去拜访一位客户，”他解释说，“我就在大厅里等他。”

“营销，”她说这个词的时候几乎有些忧伤，彼得微笑着看着她，等待着下文，“如果我上了大学的话，我就会做营销员。”她说，“我喜欢营销这份工作。”

他再一次笑了，“凯拉，”他说，把前台上她的签名读了出来，“我们达拉斯办公室有位女秘书，她自己离开了营销部，那是三年前的事了，现在她是市场经理助理，她换了两次工作。”

凯拉似乎在幻想了，他继续说，“你会用电脑吗？”“当然。”她说。

“你觉得我把你的名字放到营销部的秘书职位上怎么样？”

她笑了，“那样我就能到达拉斯去了。”

“你会喜欢达拉斯的，”他说，“我不能保证马上就有机会，但我会尽力的。”

她想，这个衣服和领带十分整洁、头发梳得整整齐齐的好人可能会让她的工作和生活发生巨大改变。

彼得穿过大厅坐了下来，打开他的便携式电脑，然后开始完成一些工作。十或十五分钟以后，他又走回了前台。“听着，”他说，“好像迈克被什么事拖住了，这里有会议室可以让我在等待的时候坐下来写电子邮件吗？”

凯拉打电话给了负责调配会议室的人并为彼得安排了一个没有登记的会议室。这里的会议室仿照了一些硅谷公司的做法（苹果也许是第一个这样做的），用卡通人物、连锁饭店、电影明星或连环漫画英雄的名字来命名。他被告知可以去用米老鼠会议室，她先帮他登记，然后给他指出了米老鼠的方向。

他找到了那个会议室，安顿下来，把他的便携式电脑连上了以太网端口。

你看到这个场景了吗？

对——这个入侵者已经在公司的防火墙内部连入局域网了。

安东尼的故事

我猜你可能会把安东尼莱克（Anthony　Lake）称为懒惰的商人，或者是近乎“古怪”的人。

他认为他应该为自己工作，而不是为别人：他想开一个商店，这样他就可以整天都待在一个地方而不用在乡下到处跑了，他想做一些肯定能赚到钱的生意。

开什么店好呢？没过多久他就决定了，他知道修车，就零配件商店好了。

怎样才能保证成功呢？他很快就想到了答案：确定零配件批发商出售给他的商品都是他想要的成本价。

他们当然不会自动说出来，但是安东尼知道怎样骗人，他的朋友米奇知道如何入侵别人的电脑，他们一起制定了一个巧妙的计划。

那天他假扮成一个名叫彼得米尔顿的员工，进入了光荣汽车零配件公司内部并把他的便携式电脑连上了他们的局域网，一切顺利，但还只是第一步，接下来他要做的事情并不容易，特别是之前安东尼为自己设置了一个十五分钟的极限时间——如果更久的话他认为被发现的风险太高了。

米特尼克信箱

不要让你的员工只看到封面就判定一本书的好坏——穿着整洁并不能为某个人带来更多的可信度。

在之前的电话中他伪装成他们电脑供应商的支持人员花言巧语地表演了一番，“你们公司购买了两年的技术支持，我们正在把你们加入数据库，这样当你们使用的某个软件程序有了补丁或是更新版本时我们就可以知道，我需要你告诉我你们使用哪些程序。”然后他得到一张程序列表，一位会计师朋友确定其中一个调用了MAS90（译者注：一款财务软件）——这个程序管理着他们的厂商列表和折扣与各自的付款方式。

有了这些关键信息，他下一步用一个软件程序扫描了局域网中所有的存活主机，没花多少时间他就找到了财务部门服务器的正确位置。从他的便携式电脑的黑客工具兵器库中，他运行了一个程序并用它来扫描目标服务器上所有的授权用户。得到了这些之后，他开始尝试了一系列常用的密码，比如“空”和“password”，“Password”起作用了，没什么好吃惊的，在选择密码的时候人们总是缺乏创造力。

才过了六分钟，游戏就完成了一半，他进入了目标服务器。

又过了三分钟，他非常小心地往客户列表里添加了他的新公司、地址、电话号码和联系人，然后找到一个至关重要的条款，在上面标明所列商品以高于光荣汽车零配件成本1%的价格卖给他。

十分钟不到，他完成了。然后他停留了足够长的时间向凯拉表示感谢，并说他仔细查看了电子邮件，了解到计划有变动，迈克塔尔伯特已经在去客户办公室开会的路上了，他也不会忘了要把她推荐到营销部门的事。

过程分析

这个自称为彼得米尔顿的入侵者运用了两次心理战术——一次是有计划的，另一次是临时准备的。

他穿得像是工资很高的管理人员，精心设计的衣服、领带和发型——这些细节看上去很小，但是它们能建立第一印象。我自己是无意中发现了这些的，以前我在加利福尼亚州GTE（译者注：美国通用电器公司）当程序员时，我发现如果有一天我没有带证件，穿着整洁但随意——比如，运动衫、休闲裤与Dockers（译者注：卡其裤经典品牌）——我就会被叫住被盘问，你的证件，你是谁，你在哪里工作？第二天我再来的时候，依然没有证件但是衣服和领带看上去非常正规，我用了一个古老的技术混入人群，和他们一起走进公司或安全入口，和他们聊天，好像我就是他们中的一员。我顺利通过了，即使警卫注意到我没有证件，他们也不会打扰我，因为我看起来像是管理人员并且还和带着证件的人在一起。

从这些经验中，我了解到应该怎样预测安全警卫的行为，像是我们中的其他人，他们会根据表面现象进行判断——社会工程师知道怎样利用这个致命弱点。

当攻击者注意到那位接待员不同寻常的努力之后，他的第二个心理战术起作用了。同时处理很多事情没有让她变得不耐烦，不仅如此，她还让每个人都觉得他们获得了她全部的注意力，他觉得这些是有上进心、想证明自己的人的标志。然后当他声称在营销部门工作时，他观察了她的反应，看他是否在她心中建立了友好的形象，他做到了。对于攻击者而言，这意味着他可以通过承诺帮她找到一份更好的工作来利用她。（当然，如果她说她想去财务部门，他就会声称自己可以在那里为她联系一份工作。）

入侵者也喜欢在这个故事里使用的另一个心理战术：用两段攻击建立信任。他首先聊到营销部的工作，然后“提到某个人”——说出另一个员工的名字——一个真实的人，顺便说一句，那的确是一个真实员工的名字。

他可以马上请求到一间会议室去，但他选择了暂时坐下来，假装在工作并等待他的同事，这样就可以避免任何可能的猜疑，因为一个入侵者是不会待在附近的。他没有待很长时间，然而，社会工程师在必要的情况下会待在犯罪现场更长时间。

米特尼克信箱

允许一个陌生人进入到可以把便携式电脑连入公司内部网络的地方，会大大增加安全风险。这对于一名员工而言非常合理，但是对于一个想要到会议室查看他（或她）的电子邮件的外部人

员，除非已经确定这名访客为可信任的员工或者网络已经被分割出来，阻止未经授权的连接，这可能是危及公司文件的薄弱环节。

必须明确指出的是：从法律的角度上看，安东尼进入大厅时，他并没有犯法；当他利用一个真实员工的名字时，他也没有犯法；当他进入会议室时，他也没有犯法；当他连入公司的内部网络并搜索目标主机时，他也没有犯法。

实际上直到他侵入了计算机系统时，他才违反了法律。

偷窥的凯文

很多年前，当我在一个小公司工作时，我注意到当我走进和其他三个人共用的IT部门办公室时，有一个特殊的人（乔，我在这里这样称呼他）会迅速地把他的电脑显示器切换到另一个窗口，我马上觉得这很可疑，当同一天发生超过两次这样的事时，我确信自己将要了解到某些事，这个人到底不想让我看见什么呢？

乔的电脑是公司小型机的终端，所以我在VAX小型机上安装了一个控制程序，这样我就可以监视他的一举一动。这个程序类似于一个在他肩膀上面的电视摄像机，把他在电脑上看到的东西精确地展示给我。

我的桌子就在乔的旁边：我可以把显示器转过来让他看不见，但是他随时都可以走过来，然后发觉我在监视他。这不是问题：他太专注于所做的事情了。

我看到的东西让我目瞪口呆，这个坏蛋调出了我的工单数据，他在查看我的工资！那时候我在那里才几个月，我猜乔是无法容忍我的工资比他高。

几分钟后我看见他在下载菜鸟黑客自己写不出来的黑客工具，这样看来乔没什么本事，并且还没有意识到美国最有经验的黑客就坐在他的右边，我觉得这很好玩。

他已经获得了我的工资信息：要阻止他已经太晚了。此外，任何电脑可以访问IRS（译者注：美国国税局）或社会保障总署的员工都可以看见你的工资。我当然不想让他发现我知道了他在干什么，我此时的主要目标是保持低调，一个好的社会工程师不会去到处宣传他的知识与才干。你通常想让人们低估你，不把你当成威胁。

所以我没有管他了，并且为乔认为他知道了我的一些秘密而暗自发笑。当这些都反过来时：我获得的信息会比他多得多。

我发现我在IT部门的三个同事全都喜欢查看这个或那个可爱秘书或（为公司里的一个女孩子）他们盯上的某位帅哥的实得工

资，并且他们还喜欢找出公司里任何令他们好奇的人（包括高层管理人员）的工资和奖金。

过程分析

这个故事说明了一个很有趣的问题，维护公司电脑系统的人可以轻易地访问工资表文件，这带来的问题是：确定谁可以被信任。在某些情况下，IT人员会在四处察看时无法避免地看到它，他们可以这样做，因为他们有特权允许他们忽略这些文件的访问控制。

一个安全措施是审核对特别敏感的文件的访问，比如工资表。当然，任何必需有特权的人都可以关闭审核或移除任何指向他们的纪录，但是每一步额外的步骤都会使不道德的员工在隐藏部分上花费更多的时间。

预防措施

从翻寻你的垃圾到欺骗安全警卫或接待员，社会工程师可以全面侵入你的公司内部，但是你会很高兴听到这里有一些你可以采取的预防措施。

临时通行证

所有上班时忘记带证件的员工都必须到大厅前台或警卫室办理一张临时证件，如果这一章第一个故事中的安全警卫在遇到没有携带员工证件的人时仔细地进行了处理，一切就会大不相同。

对于安全等级不高的公司或公司区域，也许并不需要强调每个人每时每刻都带着有效证件，但是对于公司中的敏感区域，这些就需要被严格地强制实行。必须培训员工去质疑没有佩戴证件的人，高级员工必须允许这些质疑，不去为难那些把他们叫住的人。

公司政策应该忠告那些一直没有佩戴证件的员工：他们所受的处罚可能是直接回家并且拿不到任何报酬，或者在他的个人档案上写上一笔。一些公司制定了一系列更严厉的处罚，包括向员工经理报告问题，然后发布正式警告。

另外，在有受保护的敏感资料的地方，公司应该制定在非商业时间访问的授权程序。一个解决方案是：让公司的安全部门或某个其它指定组管理这些请求，这个组将通过回电给主管或其它一些相当合理的方法来核实任何请求在非工作时间访问的员工的身份。

慎重处理垃圾

垃圾搜寻的故事揭示了公司的垃圾存在的潜在危险。

下面是八条与之相关的至理名言：

1．基于敏感程度对敏感资料进行分类。

2．在整个公司范围内建立敏感资料丢弃程序。

3．坚持在丢弃敏感信息时先将其粉碎，并使用一个安全的方法去除无法再剪碎的小纸片上的重要信息。碎纸机绝对不能处于低档粉碎状态，一个坚定的攻击者，加上足够的耐心，就可以把这些低档粉碎出来的纸片拼起来。只要很好的使用了交叉碎纸机，他们得到的就会是无用的纸浆。

4．将那些电脑媒体--软盘、Zip盘、被用来存储文件的CD和DVD、可移动磁盘、旧硬盘等--完全清除或使其无法使用，在它们被丢掉之前。记住，删除文件事实上并没有将其清除，它们还可以被恢复--就像Enron主管和其他许多人从他们的惊讶中学到的那样，把电脑媒体扔到垃圾桶里是在向当地友好的垃圾搜寻者发出邀请。（处理媒体与设备的详细指导方针见第16章）

5．在选择清洁队成员上保持适当程度的控制，如果允许的话进行后台检查。

6．周期性地提醒员工回想他们扔到垃圾桶里的资料种类。

7．锁定垃圾搜寻者。

8．对敏感资料使用分散存储空间，与可信赖的专业资料处理公司签订合同。

对员工说再见

这一点在这几页之前就谈到了，当一名离职员工想要获得敏感信息、密码、拨入号码等等时，需要执行严格的程序。你的安全程序需要提供一个多种系统的授权纪录。也许很难阻止一个坚定的社会工程师突破你的防御网，但是不要让一个离职员工都可以轻易做到。

另一个措施很容易被忽视：当一名可以从存储器恢复备份数据的员工离开时，应当为存储器调用一个写好的策略，马上通知将她的名字从授权列表中删除。

这本书的第十六章详细讲述了这个重要主题，但是在这里列出某些适当的安全措施很有帮助，就像通过那个故事强调的那样：

按照一张完整、严格的步骤列表上的内容处理一名员工的离职，对于访问过敏感数据的员工要有特殊的规定。

关闭员工的直接访问权限--最好在其离开公司之前。

不仅恢复员工ID证件需要按程序进行，任何密匙或电子访问设备也同样需要。

规定在允许任何没有安全密码的员工进入之前安全警卫要查

看他或她的照片ID，在验证列表上核实姓名，确定这个人仍是这家公司的员工。

更多的步骤对于一些公司而言未免太繁琐或太昂贵了,但是却适合一些其他的公司，下面是一些更严格的安全措施：

电子ID证件结合入口处的扫描器，当每个员工将他的证件从扫描器上划过时，电子实时判断会得出此人为当前员工并有权进入大楼。（注意，无论如何还是必须被培训安全警卫提防蒙混过关者--一个未经认证紧跟在合法员工身后的人。）

所有员工都必须在同一组内，当某个人离开时（尤其是如果这个人被解雇了）更改他们的密码。（看上去很偏激？在通用电器公司工作的那一段时间之后很多年，我了解到当太平洋电话的警卫听到通用电器公司把我解雇了时，"到处都是笑声。"但是对于通用电器公司的信任，当他们了解到一个有名的黑客曾经为他们工作时，在解雇了我之后，他们就必须更改公司里所有人的密码！）

你不想让你的公司变得像牢房一样，但是同时你需要防范那些刚被解雇就跑来想做坏事的人。

不要忘记任何人

安全警卫要注意入门级的员工，比如并不处理公司敏感信息的接待员。我们曾经在其它地方看到过，接待员是最受攻击者青睐的目标，本章中闯入汽车零配件公司的故事则是另一个例子：一个友好的穿着很专业的人，可能并不是他所声称的来自其它区域分公司的员工。需要良好的培训接待员，如何在适当的时候礼貌地请求公司ID，培训不只是针对主要的接待员，还包括每一个在午餐或下午茶时间零时坐在接待处的人。

对于公司外部的访客，需要查看其照片ID并记录信息。伪造ID并不很难，但至少严格的ID验证可以让攻击者使用电话冒充更加困难。

在一些公司，实行全程陪同访客（从大厅到会议室）的安全策略很有意义，程序应该规定陪同人员在把访客送到会面地点之前要先弄清楚这个人是员工还是非员工。为什么这很重要？因为就像我们在之前的故事中看到的那样，攻击者经常会变换角色，在大厅中表演对他们而言实在是太简单了，使接待员相信他有一个会议要参加，说，有个工程师……陪他到那个工程师的办公室……与工程师会谈之后，他才可以自由行动。

在允许一名异地员工进入之前，必须履行适当的程序，确认此人真的是公司的员工。接待员和警卫必须要了解攻击者伪造身份所使用的方法。

怎样阻止攻击者进入大楼并把便携式电脑连入公司的内部网络？拜当今的技术所赐，这的确是个挑战：会议室、培训室和其它类似的地方都不应该留下不安全的网络端口，应使用防火墙或路由器将其保护起来，但更好的做法是使用安全的方法对任何连入网络的用户进行识别。

保护IT部门！

忠告：在你的公司里，IT部门的每一位员工或许都知道（或能花几分钟时间找出）你的收入、CEO的实得工资和谁用了公司的钱去滑雪度假。

在一些公司甚至有可能出现IT人员或会计人员给他们自己加工资、向一个伪造的卖家付款、删除人力资源档案中消极的评价等情况。有时候只是因为担心被抓住，他们才没有那样做，直到有一天，某个贪婪或本性不诚实的人冒着风险做了所有他认为能免于责罚的事情。

这里当然也有解决方案，可以通过配置严格的访问控制来保护敏感文件，所以只要验证访问者有权打开它们。有一些操作系统的审核控制能设定保留事件的日志，比如每一个试图访问敏感文件的人（无论是否访问成功）。

如果你的公司了解了这一问题并恰当地实现了对敏感文件的访问控制与审核--你就在正确的方向上迈出了强有力的一步。

# 第十一章 综合技术与社会工程学

社会工程师可以通过操纵人们来达到目标，但也常常需要很多关于电话系统和电脑系统的知识与技能。

下面是一个典型的社会工程学案例，其中技术起着至关重要的作用。

铁窗下的入侵

哪里有最可靠的防范物理、电讯或电子入侵的安全设备？诺克斯堡（美军基地）？当然。白宫？那还用说。隐藏在一座山下面的北美防空联合司令部（NORAD）？毋庸置疑。

那联邦监狱和青少年拘留中心怎么样？应该和这个国家的其它地方一样安全吧，对吗？很少有人逃跑，当他们这样做时，通常会在很短的时间内被抓回来。如果你认为联邦机构对社会工程学攻击免疫，那你就错了——绝对的安全是不存在的，无论是哪里。

几年前，有两个骗子（职业骗子）从一个本地法官手里弄到了一大笔现金，两个人这些年断断续续地触犯了很多次法律，但这一次他们引起了联邦当局的注意。他们抓住了其中的一个骗子，查尔斯康多尔夫（Charles Gondorff），把他关进了圣地亚哥附近的拘留中心。联邦官员认为他有脱逃风险并对社会构成了威胁。

他的搭档乔尼胡克（Johnny Hooker）知道查尔斯会需要一个辩护律师。但是钱从哪里来名牌服装、特殊爱好、女人，像大部分骗子一样，他们的钱来得快去得也快。乔尼几乎都养不活自己了。

为了有足够的钱请到优秀的律师，乔尼不得不实施另一次骗局，但他无法单独完成，查尔斯康多尔夫在他们以往的行骗中总是扮演着智多星的角色，不过乔尼并不害怕到拘留中心去问查尔斯该怎么做，只要不让Feds（译者注：FBI特工）知道有两个人在那里策划骗局并且非常热心地帮助对方。值得注意的是，只有家属才能探监，这意味着他不得不伪造一张证明来声称自己是一个家庭成员。试图在联邦监狱使用伪造ID听上去可不是个明智的决定。

不，他可以通过其它途径与康多尔夫取得联系,只是不太容易。联邦、州或地方监狱都不允许囚犯接听电话，联邦拘留中心每一部电话上都贴有这样的标签：“忠告用户，此电话允许监听，使用即同意。”在政府官员监听的电话里谈论如何犯罪只会延长你的联邦基金假期。乔尼知道有些电话是不被监听的：比如，囚犯与他的律师之间的通话（委托人与律师的通信受宪法保护）。事

实上，康多尔夫所在的监狱有电话可以直接联系联邦公共辩护处（PDO），拿起那些电话便能直接与PDO连线，电话公司把这种服务称为“直通”。这种服务被认为是安全的、不受攻击的，因为它只能呼出到PDO，并且锁定了呼入线路，即使某个人不知怎么的弄到了电话号码，也会被电话公司“呼叫拒绝”（一个笨拙的电话服务术语）。

在所有半路出家的骗子精通欺骗的艺术之前，乔尼找到了解决这个问题的办法。在监狱里，康多尔夫拿起某部PDO电话：“我是汤姆，电话公司修复中心。”

术语

直通：电话公司术语，当电话被拿起时接通一个特殊的号码。

呼叫拒绝：电话公司的一个服务选项，设置某个电话号码无法呼入。

“我们正在对这条线路进行测试，我需要你拨9，然后拨0、0。”9是转到外部线路，00是接通一个长途接线员。如果接电话的PDO员工熟知这种骗局，就不能用这种方法了。

乔尼还有更好的办法。他很快了解到拘留中心有十个房间单元，每一间都有公共辩护处的直通电话线路。乔尼遇到了一些障碍，但他就像是一名社会工程师，总能想办法解决这些烦人的问题。康多尔夫在哪个单元？那个单元的直通服务号码是多少？他最初怎么样给康多尔夫留言而不会被狱警拦截呢？

也许这在普通人看来是不可能的，比如获得联邦公共机构的秘密电话号码，一名欺骗艺术家通常只需要打几次电话就可以了。翻来覆去地思考了几个晚上，乔尼把所有事情都想到了，他的计划总共五步。

首先，找到那十部PDO直通电话的电话号码。

更改那十部电话的设置使其允许呼入。

找出康多尔夫所在的单元。

然后找到该单元的电话号码。

最后，他就可以和康多尔夫进行预期的通话了，不会引起政府的任何怀疑。

小菜一碟，他想。

呼叫Ma Bell（AT&T）...

乔尼冒充总务管理局的工作人员打电话到电话公司商业办公室（该部门负责向联邦政府销售产品与服务），说他正在处理一张附加的服务订单，需要知道当前使用的所有直通服务的账单信

息，包括圣地亚哥拘留中心使用中的电话号码和月账单。那位女士非常高兴地给予了帮助。

为了进行确认，他试着拨入了其中一条线路并收到了典型的语音提示，“此线路已断开或不在服务区”——他知道这意味着线路锁定了呼入，和他预想的一样。

他十分了解电话公司的运转程序，下一步他需要联系近期记忆修改授权中心（RCMAC，我总是惊讶于取这种名字的人！）。他打电话到电话公司商业办公室，谎称自己是维修中心办公室的，需要知道RCMAC的号码来处理某个地区号和前缀所在的服务区，该中心办公室也负责分配拘留中心的呼入线路。这属于常规请求，相关规定允许在一定范围内向技术人员提供一些帮助，那位员工毫不犹豫地把号码给了他。

他拨通了RCMAC的电话，使用一个假冒的名字，伪装成维修中心的工作人员，说他收到一位女士的投诉，有一个他负责的电话号码一直不能呼入，乔尼问：“这个号码被设置为呼叫拒绝了吗？”

“是的。”她说。

“好的，这就解释了为什么那位客户接不到电话！”乔尼说，“听着，你能不能帮我个忙，修改那条线路的类型代码或删除呼叫拒绝类型，好吗？”

当她在另一个电脑系统上查看是否允许更改服务状态时停顿了一下，她说，“此号码受限制为只能呼出电话，没有服务命令。”

“是的，这是个错误，我们昨天就应该处理的，但是通常处理这些的员工因病回家了，她又忘了拜托别人，所以现在那位客户理所当然地对这件事情非常不满了。”

短暂的停顿，那位女士在考虑这个超出常规并违反了标准操作程序的请求，她说，“好吧。”

他可以清楚地听到她在输入修改，几秒钟就完成了。

坚冰被打破了，他们之间建立了一种合作关系，看到这位女士如此配合的给予帮助，乔尼毫不犹豫地选择了更进一步，他说，“你能再多花几分钟帮帮我吗？”

“可以，”她回答道，“还有什么事吗？”

“我有几条属于同一个客户的其它线路，全部都是一样的问题，我把号码读出来，只要确认它们没有被设置为呼叫拒绝就可以了——好吗？”她说好的。

几分钟后，十条电话线路全都被“修复”为允许呼入电话了。

寻找康多尔夫

下一步，找到康多尔夫所在的房间单元，这一信息显然是管理拘留中心和监狱的人不想让外部人员知道的，乔尼再一次使用了他的的社会工程学技术。

他打电话到了另一个城市的一座联邦监狱——他选择了迈阿密——声称他从纽约拘留中心打电话来。他请求和监狱里使用岗哨电脑的人谈话（该电脑系统包含了所有的囚犯信息，全国的监狱机构都能访问）。

当和那个人连上线时，乔尼换上了他的布鲁克林口音，“你好，”他说，“我是纽约FDC（联邦拘留中心）的托马斯，我们到岗哨的线路总是不能用，你能帮我找出这个囚犯的位置吗？我想这个囚犯在你们那里。”然后读出康多尔夫的名字和他的注册号。

“不，他不在这里，”过了一会儿那个人说，“他在圣地亚哥的拘留中心。”

乔尼假装成很吃惊的样子，“圣地亚哥！上个礼拜他就应该被“马歇尔空运”到迈阿密的！我们说的是同一个人吗——他的DOB（date of birth 出生日）是哪一天？”

“12/3/60。”这个人看着他的屏幕上读道。

“是的，是同一个人，他在哪个房间单元？”

“他在北十号。”这个人愉快地回答着问题，即使没有任何合理的理由解释为什么一个纽约的监狱员工需要知道这些。

现在乔尼知道了康多尔夫所在的房间单元，下一步就要找出哪一个是北十号单元的电话号码。

这一步有点困难，乔尼拨打了其中一个号码，他知道那些电话的扬声器已经被关掉了，没有会知道它在响。于是他坐在那里一边看欧洲名城旅游指南，一边听着扩音器传出的持续不断的铃声，直到最终某个人把它拿起来。那个囚犯在电话的另一端当然是想要联系上他的法庭指定律师，乔尼已经准备好预期的回应了。“公共辩护办公室。”他声称道。

当那个人寻求他的律师时，乔尼说，“如果他在的话我会看见的，你是从哪个房间单元打过来的？”他草草记下了这个人的回答，放下电话，片刻之后回来说，“他在法院，你只能稍后打来了。”然后挂断。

他花了大半个早晨的时间，但还算幸运：第四次尝试就找到了北十号，现在乔尼知道了康多尔夫所在房间单元的电话号码。

时间同步

现在要通知康多尔夫接电话的时间，这比听上去要更容易。

乔尼用他的官方语调打到拘留中心，声称自己是一名员工，请求转接到北十号。然后当那名狱警拿起电话时，乔尼使用了犯人物品保管室（Receiving and Discharge，该部门负责接收和释

放囚犯）的内部缩写，“我是R&D的泰森，”他说，“我需要和囚犯康多尔夫说话，我们要寄出他的一些财物，需要询问他地址，你能把他叫过来接电话吗？”

乔尼可以听到那名狱警在值班室里大喊大叫，焦急地等待了几分钟之后，熟悉的声音从电话那头传来。

乔尼对他说，“在我解释之前不要说话。”乔尼解释了这个骗局，然后说，“如果你可以在今天下午一点使用公共辩护办公室的直通电话，就不要说话，如果不能，那么说个你可以到那里的时间。”康多尔夫没有回答，乔尼继续说，“好的，一点到那里，到时候我会打电话给你，拿起电话，如果听到呼出的声音就迅速挂断，每过20秒试一次，直到听到我的声音为止。”

下午一点，康多尔夫拿起了电话，乔尼已经在等他了，他们进行了一次轻松、愉快、悠闲的谈话，在一连串类似的电话里设计骗局为康多尔夫筹措律师费——所有这些都不受政府的监视。

过程分析

这个有趣的故事提供了一个关于社会工程师怎样通过几个独立的、看似不合理的骗局让表面上不可能的事情发生的很好的例子。在现实中，每一步都会有一些小小的问题，直到完成整个骗局。

第一个电话公司的员工认为她在向联邦政府总务管理局的某个人提供信息。

第二个电话公司的员工知道她不应该在没有服务命令的情况下更改电话服务类型，但还是帮助了这个友好的人。这让呼入拘留中心的十条公共辩护电话线路成为可能。

对于那个在迈阿密拘留中心的人而言，帮助某个遇到电脑故障的联邦机构人员似乎是非常合理的，即使没有任何理由可以解释为什么他需要知道房间单元，为什么不问一问？

还有北十号的那个狱警，他相信这个打电话的人和他是同一个机构的，为了工作上的事情？这是非常合理的请求，所以他叫来了囚犯康多尔夫，这没什么大不了的。

周详的计划让整个骗局顺利地完成了。

快速下载

在法学院毕业十年之后，耐德拉辛（Ned Racine）发现他的同班同学全都住进了带草坪的别墅，成了乡村俱乐部的一员，每星期打一次或两次高尔夫，而他则在为没有足够的钱付帐单的人处理微不足道的案件。嫉妒一直折磨着他，终于有一天，耐德受够了。

他曾经有过的唯一个好客户是一家很小但很成功的会计公司，这家公司擅长于收购和兼并。他们雇用耐德的时间不是很

长，但足够让他了解他们涉及的那些生意，一旦他们被媒体报道，将会有一家或两家上市公司的股票价格受到影响。小打小闹，可以通过交易板购买股票，但是使用一些方法会更好——只要少量地投入资金就可以获得丰富的回报。如果他可以接触到他们的文件并找出他们正在研究的那些股票……

他通过一个朋友认识了一个特殊的人，这个人听了他的计划之后为之叫绝并同意向他提供帮助。为了一笔比平时少得多的酬金（和耐德在股票市场上赚的钱不成比例），这个人对耐德进行了指导，还给了他一个随身携带的微型设备（崭新的行货）。

在接下来的几天里，耐德一直监视着那家会计公司朴实无华、店面一样的办公室所在的小型商业停车场，大部分人在5点30到6点离开，到了七点，停车场就已经空了，清洁工在7点30左右出现，好极了。

第二天晚上8点之前几分钟，耐德把车停在了停车场的街对面，和他预期的一样，停车场只剩下清洁服务公司的卡车了。耐德把耳朵贴在门上，听到真空吸尘器运作的声音，他把门敲得很响，然后站在那里等待，他穿着西装，手里还拿着他的旧公文包。没人应门，他很有耐心地又敲了一次，终于来了一个清洁工。“你好！”耐德隔着玻璃门大喊，然后拿出他之前弄到的一个股东的名片，“我把钥匙忘在车里了，我要到我的桌子上拿点东西。”

那个人打开门让耐德进来，再把门给锁上，然后把走廊上的灯都打开了，这样耐德就可以看清路了。好的——他很喜欢这个把食物端到他桌子上的人，大概他把每一个理由都想过了。

米特尼克语录

商业间谍和电脑入侵者有时候会进入现实中的目标公司。比用铁锹闯进去要好得多，社会工程师运用欺骗的艺术让人们为他开门。

耐德打开了一个股东的电脑，当它启动的时候，他把一个微型设备（小到可以挂在钥匙圈上的玩意儿，但是可以存储超过120MB的数据）插在了电脑的USB端口上。他用这个股东的秘书的用户名和密码（很方便地用便签贴在了显示器上）登陆了网络。不到五分钟，耐德下载了每一个存储在工作站和网络目录上的电子表格与文档文件，然后回家了。

轻松赚钱

当我第一次在中学时代接触电脑时，我们只能通过调制调解器连入洛杉矶市区的一台L.A（洛杉矶缩写）所有中学共用的中心DEP PDP II小型机，电脑上的操作系统叫做RSTS/E，那是我学会使用的第一个操作系统。

1981年，那时候，DEC为他的产品用户每年主办一次研讨会，有一年我了解到研讨会将在L.A举办。一家热门杂志为此操作系统的用户公布了一个新的安全产品，LOCK-II，这个产品有一个像这样的很有创意的广告："现在是3:30，M和乔尼正在沿街寻找你的拨入号码，555-0336，这已经是第336次了。你入他出，选择LOCK-II。"这个广告暗示该产品能防止黑客入侵，这一次的研讨会把它展示出来。

我很想亲自看看这个产品。我在中学的伙伴和朋友，文尼（我曾经的入侵搭档，后来成了抓我的联邦密探），和我一样对新的DEC产品充满了兴趣，他怂恿我和他一起去研讨会。

现金悬赏

我们到了那里发现已经有一大群人围着LOCK-II的展台了，似乎开发者设下了现金悬赏，打赌没人能入侵他们的产品，这对我而言实在是难以拒绝的挑战。

我们把头伸直了往LOCK-II展台里面看，发现有三个此产品的开发者正在操作它，我认识他们，他们也认识我——我那时已经是小有名气的电话盗打者和黑客了，洛杉矶时报报导了我初次尝试社会工程学欺骗的故事，半夜闯进太平洋电话中心，在警卫的鼻子底下拿走电脑手册。（洛杉矶时报为了让报导更有吸引力而公布了我的名字：因为我还是青少年，所以这违反了隐匿未成年人姓名的法律规定。）

当我和文尼走进去的时候，气氛变得微妙起来，因为他们通过报纸了解到我是个黑客，看到我的出现有些震惊，而我们则是看到他们每个人所在的展台上各贴着100美金的悬赏，只要侵入他们的系统就能获得整整300美金——对于两个青少年而言这是一笔巨额财富，我们都等不及要开始了。

LOCK-II被设计为具有双层安全验证，用户必须要有一个合法的ID和密码，在特殊情况下此ID和密码只能从被授权的终端登陆（这称为终端基础安全）。要入侵这个系统，黑客不仅要知道一个账户ID和密码，还需要从合法的终端登陆。这是个很好的安全规则，LOCK-II的发明者深信它能抵挡入侵，我们决定给他们上一课，然后将三百美元收入囊中。

我认识的一个人（RSTS/E的头头）已经在展台打击我们了，几年前他和其他一些家伙向我发出过入侵DEC内部计算机的挑战

——在他的搭档让我进去之后，多年以后他成了受人尊敬的程序员，他在我们到达之前就已经尝试过攻击LOCK-II的安全程序了，但没有成功，这让开发者对他们的产品安全更有信心了。

术语

终端基础安全：基于特定的计算机终端作为安全验证：这一做法在IBM大型计算机中非常流行。

比赛很简单：入侵，赢得美金，一场公开的惊人表演……除非有人能打败他们并拿走钱。他们非常相信他们的产品，甚至还在展台上勇敢地公布了系统中的一些账户名称和相应的密码，不只是普通账户，还包括所有的特权账户。

这其实没有听上去的那么勇敢：我知道，在这种设置类型中，每台终端都插在计算机自身的一个端口上，不难断定他们已经设置了这五台终端只能从非系统管理员权限登陆。看来似乎只有两条路：要么完全突破安全程序（这正是LOCK-II被设计来防范的），要么用开发者难以想象的某种方法绕路而行。

接受挑战

文尼和我一边走一边讨论，然后我说出了我的计划……我们在四周徘徊着，隔着一段距离注意着展台。午餐时间，当人群稀疏的时候，那三个开发者会利用这一间隙一起出去吃东西，留下了一个可能是他们中某个人的妻子或女朋友的人，我们走了回去，为了转移那位女士的注意力，我和她聊起了天，“你在这家公司多久了？”“你们公司还有哪些销售的产品？”等等。

趁此机会，文尼离开了她的视线，他和我同时开始了行动。除了着迷于计算机入侵和我对魔术感兴趣以外，我们都秘密地学习了怎样开锁。作为一个小孩子，我读遍了圣费尔南多谷一家地下书店中关于开锁、解手铐和伪造身份证的书籍——所有这些都不是一个小孩子应该知道的。

文尼和我一样练习了很多次开锁，直到我们能完美地解决所有普通的五金商店的锁为止。有一段时间我沉迷于开锁的恶作剧，比如戏弄为了安全而使用两把锁的人，把锁拿下来，互换位置放回去，这样那个人在用错误的钥匙开锁时会变得不知所措。

展厅里，我继续打扰着那位年轻女士，文尼闪到展台后面打开了他们安放PDP-11小型机和电线电缆的柜子上的锁。锁匠上这把锁更像是在恶作剧，这是圆片锁，像我们这样笨拙的业余开锁爱好者都能轻易地撬开它。

文尼花了整整一分钟时间才把锁打开，在柜子里他找到了我们所期望的东西：接入用户终端的插线集和一个控制终端端口，这是计算机操作员或系统管理员用来控制所有计算机的终端，文尼把展台上某台终端插在了控制端口上。

这意味着这台终端现在已经被认为是控制终端了，我走过去用开发者提供的密码登陆了进去。因为LOCK-II的程序现在已经认为我是从授权终端登陆的，所以它同意了我的访问，并且我拥有的是系统管理员权限。我给操作系统打了个补丁，让我能用特权用户登陆展台上的任意一台终端。

我一安装完补丁，文尼就马上回去断开了终端连线并把它插回了原处，然后他又把锁拿了下来，不过这一次是把柜门关上锁好。

我把目录列举出来想看看这台计算机上有些什么文件，在查找LOCK-II程序和相关的文件时我无意中发现了一些让人大吃一惊的东西：一个不应该出现在这里的目录。开发者太自负、太确信他们的软件是无敌的了，以至于没有移除这个新产品的源代码。走到邻近的硬拷贝终端前，我开始把一部分源代码打印在当时使用的长条带电脑纸上。

当那些人吃完饭回来时文尼正好和我会合了，他们发现我正坐在计算机上敲击按钮，而打印机还在继续转动。“你在做什么？凯文？”他们中的一个人问。

“啊，只不过是在打印你们的源代码。”我说。当然，他们认为我在开玩笑，直到他们看向打印机时才发现那是真的，那是他们被严密保护的产品源代码。

他们不相信我用特权用户登陆了。“输入T命令看看。”其中一个开发者说，我照做了，接下来屏幕上的显示证明了一切。那个人拍打着他的前额，然后文尼说，“三百美金，谢谢。”

米特尼克语录

这是另一个聪明人轻视敌人的例子。那你呢？你对自己公司的安全措施很有信心吗？你愿意用300美金打赌吗？有时候通往安全设备的路并不像你想象的那样只有一条。

他们给了钱，文尼和我围着展台转悠了一天，我们的证件上贴着百元的美钞，每个看见这些钞票的人都知道它们意味着什么。

当然，文尼和我没有攻破他们的软件，并且如果开发小组为比赛设定了更好的规则，或用了真正安全的锁，或者小心地看管了他们的设备，他们那天也不会经历这样的屈辱——出自两个青少年之手。

我后来了解到开发小组去银行取了些现金：那些百元美钞是他们身上所有的零钱。

入侵工具字典

当某个人拿到了你的密码，他就能入侵你的系统，在大多数情况下，你甚至不知道发生了什么事。一个名为伊凡彼得斯的年轻的攻击者把目标锁定在了一款新游戏的源代码上，他可以轻易地进入那家公司的广域网，因为他的一个黑客伙伴已经攻陷了那家公司的一台Web服务器。在找到一个未修补Web服务漏洞之后，他的朋友差一点从椅子上摔下来，因为他发现这个系统被设置成了双定位主机，这意味着他得到了一个内部网络的入口。

但是当伊凡连接的时候，他遇到了一个类似于在罗浮宫寻找蒙娜丽莎的挑战，没有建筑平面图，你能走上数星期。这是家环球公司，有好几百个办公室和数千个电脑服务器，并且他们没有提供精确的开发系统索引或服务漫游指南来引导他到达正确的服务器。

伊凡无法使用技术手段找出目标服务器的位置，作为替换，他选择了使用社会工程学。他用类似于这本书中其他地方提到的方法打起了电话，首先，打到IT技术支持部门，声称自己是公司的员工，他的团队为产品设计了一个界面，然后询问游戏开发团队项目经理的电话号码。

接着他伪装成IT部门的人打给那个部门经理。“今天晚上，”他说，“我们要更换一个路由器，需要确认你的团队里的人是否能连接你们的服务器，所以我们想要知道你的团队用的是哪个服务器。”网络始终处在受保护状态，给出服务器的名称不会伤及任何东西，它是受密码保护的，服务器名称不会帮助任何人入侵，所以这个人把它告诉了攻击者。没有麻烦地回电话验证他所说的事情，或写下他的名字和电话号码，他直接给出了服务器名称，ATM5和ATM6。

密码攻击

在这里，伊凡需要通过技术手段获取验证信息，大多数系统攻击的第一步都是远程扫描出一个弱口令账户，这是进入系统的最初入口。

当攻击者尝试远程扫描密码时，这可能需要他在几个小时里保持与公司网络的连接，他这样显然是在冒险：时间越长，被发现和被抓住的风险越高。

作为一个预备的步骤，伊凡需要列举出目标系统的详细资料，因特网又一次方便地提供了相应的软件（http://ntsleuth.0catch.com：“catch”之前是数字0）。伊凡找到了几个

在互联网上公布的自动列举进程的黑客工具，这样就避免了手动操作引起的麻烦（时间过长导致风险过大）。伊凡知道大多数公司使用的都是基于Windows的服务器，他下载了一个名为NBTEnum的NetBIOS（BIOS：基本输入输出系统）列举工具。他输入了ATM5服务器的IP（Internet protocol，Internet协议）地址，然后开始运行程序。列举工具能扫描出服务器上存在的账户。

术语

列举：查看操作系统已启动的服务并列出允许访问系统的用户的账户名。

一旦扫描出存在的账户，可以使用同一个列举工具对计算机系统进行字典攻击，这是许多计算机安全人员和入侵者非常熟悉的，但大多数其他人可能在了解之后会感到震惊，这种攻击使用常用单词对系统上每个用户的密码进行尝试。

在某些事情上我们都很懒，但我总是惊讶于人们选择的密码，他们的创造力和想象力似乎都消失了。我们中大多数人都想要一个安全系数高又容易记忆的密码，这通常意味着一些和我们有联系的东西，例如我们名字的首字母、中名、昵称、配偶的名字、喜欢的歌、电影或饮料，我们住的街道或生活的城镇、驾驶的车型、喜欢的夏威夷滨海乡村、常去钓鲑鱼的河流。看出这里的模式了吗？全都是人名、地名或字典上的常用词。字典攻击可以非常迅速地把常用单词当成密码去尝试一个或多个用户账户。

伊凡是分三个阶段进行的字典攻击，第一次，他尝试了一张包含800个常用密码的列表：列表还包括隐私和工作。这个程序也可以在每个单词的前后添加数字或当前月份。程序尝试了每一个扫描到的账户，运气不好，没有成功。

第二次尝试，伊凡进入Google搜索引擎搜索“单词列表 字典”并找到了数千个包含大量单词列表和字典的站点。他下载了一整部电子英语字典，然后他用许多在Google上找到的单词列表将其扩充。伊凡选择了http://www.outpost9.com/files/WordLists.html。

这个站点允许他下载（全免费）的一系列文件中包含了姓氏、教名、国会名、演员名、还有圣经中出现的单词和名字。

其它许多站点提供的单词列表实际上来自于牛津大学ftp://ftp.ox.ac.uk/pub/wordlists。

在其它站点提供的列表中有卡通动画的名称，有《莎士比亚》、《奥德赛》、《托尔金》、《星际旅行系列》和《科学与信仰》中出现的单词，等等。（有一家在线公司以20美元的低价

出售包含440万个单词和名称的列表。）攻击程序可以设置将字典中的单词顺序颠倒，另外——这也是许多电脑用户认为能加强安全的做法。

比你想的更快

一旦伊凡选定了使用的单词列表，软件就会自动开始攻击，这样他可以把注意力放在其它事情上了。这是难以置信的一部分：你可能认为这样的攻击可以让黑客去做里普·万·温克尔的大梦（译者注：美国作家华盛顿·欧文在其小说《里普·万·温克尔》中叙述主人公里普·万·温克尔在山中一睡20年,醒来发现世事全非）了，当他醒来的时候软件进度条才会涨一点点，但事实上，依赖于被攻击的平台、系统安全配置和网络连接质量，尝试完一本英语字典里所有的单词，难以置信，只要不到三十分钟！

当攻击正在进行的时候，伊凡打开了另一台电脑对开发小组使用的另一台服务器（ATM6）上进行了类似的操作。二十分钟后，攻击软件完成了大多数毫无防范的用户认为不可能的任务：它破解了一个密码，软件显示某个用户选择了密码“Frodo”，《魔戒》中一个矮人的名字。有了这个密码，伊凡就可以登陆ATM6服务器了。

对于我们的攻击者而言有一个好消息和一个坏消息，好消息是他破解的账户拥有管理员权限，这是进行下一步的基础，坏消息是游戏的源代码怎么也找不到。最终可以肯定它在ATM5上，而针对ATM5的字典攻击没有成功，但是伊凡没有就这样放弃，他还有一些更多的方法可以尝试。

在一些Windows和UNIX操作系统上，他们存放密码哈希值（加密的密码）的地方可以被任何访问此计算机的人查看，理由是加密密码无法破解因此不需要保护。这种说法是错的，使用另一个同样可以在因特网上找到的叫做pwdump3的工具，他可以从ATM6中提取出密码哈希值并将其下载。

密码哈希值文件示例：

Administrator:

500:95E4321A38AD8D6AB75EOC8D76954A50:2E48927AO
BO4F3BFB341E26F6D6E9A97 : : :

akasper :

1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357
F157873D72D0490821: : :

digger:
1111:5D15COD58DD216C525AD3B83FA6627C7 :
17AD564144308B4 2B8403DOIAE256558: : :

ellgan :

1112:2017D4A5D8D1383EFF17365FAFIFFE89:O7AEC950C22CBB9
C2C734EB89320DB13: : :

tabeck:
1115:9F5890B3FECCAB7EAAD3B435B51404EE:
1FO115A72844721 2FCO5EID2D820B35B: : :

vkantar :

1116:81A6A5DO35596E7DAAD3B435B51404EE:B933D36DD12258
946FCC7BD153F1CD6E : : :

vwallwick:
1119 :
25904EC665BA30F4449AF42E1054F192:15B2B7953FB6
32907455D2706A432469 : : :

mmcdonald:
1121:A4AEDO98D29A3217AAD3B435B51404EE:
E40670F936B7 9C2ED522F5ECA9398A27 : : :

kworkman :
1141:C5C598AF45768635AAD3B435B51404EE:
DEC8E827A1212 73EFO84CDBF5FD1925C : : :

现在有了下载到电脑上的哈希值，伊凡要用另一种风格迥异的暴力破解工具对所有的数字、字符和特殊符号组合进行尝试。

伊凡使用的软件工具叫做L0phtcrack3（loft-crack出品，位于www.atstake.com，另外在www.elcomsoft.com中有几个很好的密码恢复工具），系统管理员用L0pht-crack3检查弱口令1，攻击者用它来破解密码。LC3暴力破解对密码的尝试包括字母、数字和大部分的符号组合！@#$%^&，它能系统地尝试大多数字符的每一个种可能组合。（注意，如果使用的是无法显示的字符，LC3也

无法将其破解）

这个程序有着难以置信的速度，在1GHz处理器的机器上最高能达到每秒尝试280万次，即使是这样的速度，如果系统管理员恰当地配置了Windows操作系统（关闭LanMan哈希值的使用），破解一个密码仍然要消耗大量的时间。

术语

暴力破解：通过尝试每一种可能的字母、数字、符号组合对密码进行破解。

因此攻击者通常会下载哈希值并在他的（或其他人的）机器上进行攻击，这样就不需要保持和目标公司网络的连接，也没有被发现的风险。

对于伊凡而言，这样的等待不算漫长。几个小时后，他得到了每一个开发小组成员的密码，但这些是ATM6上的用户密码，并且他已经知道游戏源代码不在这个服务器上了。

现在怎么办？他还是没有得到ATM5上某个账户的密码。根据他对典型用户脆弱的安全习惯的理解，他认为某个小组成员可能会在两个服务器上选择同样的密码。事实上，他真的找到了，某个小组成员在ATM5和ATM6使用的密码都是“garners”。

大门向着伊凡敞开了，他自由地搜寻着他想要的程序，直到他找到了源代码的目录并愉快地下载了下来，然后他进行了系统入侵中典型的一步：他修改了一个隐匿用户（管理员权限）的密码，以防将来想要获得软件的更新版本。

过程分析

上述攻击利用了技术和人的弱点，攻击者首先用电话骗局获得了目标信息所在服务器的位置和主机名，然后他用工具扫描出了所有的有效账户名，接着他进行了两次连续的密码攻击，其中有一次是字典攻击（使用英语字典中的单词搜索常用密码，有时还会增加包含姓名、地名和特殊爱好的单词表）。

因为任何人都能获取商业的和公共流通的黑客工具（无论出于何种目的），所以对企业计算机系统和基础网络的保护显得更加重要。

当然，这种威胁不能被夸大，《计算机世界》杂志针对奥本海默基金公司的分析得出了惊人结论。公司的网络安全与灾难恢复副主管用标准软件包进行了一次密码攻击，杂志报导说他只用了三分钟就得到了800个员工的密码！

米特尼克语录

在大富翁（Monopoly）游戏的术语中，如果你使用一个常用单词作为你的密码——就直接去了监狱，不能前进，不能收取200美金的租金（译者注：在大富翁中，如果你第三次掷出相同的点数，就会被立刻送进“监狱”）。你需要告诉你的员工怎样选择密码，真正地保护你的资产。

预防措施

当攻击者在攻击中添加了技术元素时，社会工程学攻击可以变得更加具有破坏性，抵挡这种攻击的常用方法是在人和技术两方面同时采取措施。

就说不

在这一章的第一个故事中，电话公司RCMAC的员工不应该删除掉十号电话线路的呼入拒绝状态，因为没有服务命令批准进行修改。只让员工了解安全程序和规定还不够，还应该让他们知道这些规定对于公司的安全而言有多么重要。

应当阻止重要系统中违反安全程序的行为，当然，安全规定必须结合实际，过于繁琐的规定会被员工无视的。同样，安全认知程序需要让员工们了解，因为急于完成手头上的工作而绕过必要的安全程序会伤害到公司和同事。

同样的警告也应该出现在向电话上的陌生人提供信息的时候，无论这个人怎样花言巧语地介绍自己，也不管他在公司中有何地位和资历，在确认呼叫者的身份之前，绝对不能向他提供任何非公共信息。如果严格遵守了这一规定，这个故事中的社会工程学骗局就不会成功，联邦囚犯康多尔夫也无法和他的搭档乔尼商讨新的骗局。

我在这本书中反复强调了一点：验证，验证，还是验证。在没有确认请求者的身份之前，不能响应他的任何请求--就这样。

正在清理

对于没有安全警卫昼夜值班的公司而言，如何阻止攻击者在下班以后"拜访"办公室？清洁工会像往常一样对待似乎是公司员工的任何人，毕竟，那些人可以找他们的麻烦或解雇他们。因此，不管清洁队是公司内部的还是从外部中介机构签约的，都必须接受物理安全事件培训。

清洁工作当然不会需要大学文凭，也不需要英语能力和常规训练，只要知道一些非安全的东西比如怎样使用清洁产品进行不

同的作业就可以了。"如果有人想在下班时间进来，你要查看他们公司证件，然后打电话到清洁公司办公室解释情况，等待批准。"一般这些人是不会收到这样的指令的。

一家机构应该在发生这种情况之前有所防范并以此来培训员工。在我的个人经验里，我发现大多数（而不是全部）的私营商业部门在物理安全方面非常松懈。你可以用另一种方式解决问题，把责任交给你的公司员工。没有24小时警卫服务的公司应当告诉它的员工，如果要下班后进入公司，就带上他们自己的钥匙或电子访问卡，能否进入不能让清洁工来决定。然后要求清洁公司培训他们的员工，在工作的时候不放任何人进来，这是个简单的规定：不要为任何人开门。适当的话，可以把它作为条款写在与清洁公司的合约里。

同样，清洁队应当接受识别蒙混过关者（跟随合法员工通过安全入口的人）的培训，不允许其他人（就算那个人看上去是一名员工）跟随他们进入大楼。

偶尔（比如，一年三到四次）也要更进一步安排渗透测试或攻击评估，在清洁队工作的时候让某个人站在门外尝试进入大楼。你可以聘请专业公司的人员进行渗透测试，这比用你自己的员工要好。

传递它：保护你的密码

越来越多的机构更加重视通过技术手段加强安全策略了--比如，对操作系统进行配置，强化密码策略，限制非法登陆尝试（超过一定次数则锁定账户）。事实上，Microsoft Windows商业平台一般都包含有这些功能。尽管如此，繁琐的操作还是很容易给用户带来烦恼，这些产品的安全功能通常都被关闭了。真实情况是软件厂商把产品的安全功能默认设置为关闭了，正确的做法应该恰恰相反。（我猜他们很快就会明白了。）

当然，公司的安全策略应当规定系统管理员在所有可能的情况下通过技术手段强化安全策略，达到不过分依赖人为操作的目的。你可以轻易地限制特殊账户的连续无效登陆尝试次数，这样，攻击者的生活显然变得更困难了。

所有的机构都面临着高度安全和员工生产力之间的平衡问题，这导致了一些员工无视安全策略，不接受保护公司敏感信息的最基本的安全措施。

如果一家公司的策略中留有未标明的地方，员工可能会按照最低标准执行，这样会很方便并让他们的工作变得轻松，一些员工会拒绝变动并公然地漠视好的安全习惯。你可能会遇到这样的一个员工，他遵守了关于密码长度和复杂性的规定，但是又把密码写在便签上，然后贴在他的显示器上。

保护你的公司安全的至关重要的一部分是，使用高强度的密码，在技术上与合理的安全配置结合起来。

对密码策略的详细讨论，请看第16章。

# 第十二章 攻击新进员工

正如这里的许多故事讲述的那样，在机构中处于低层的员工常常成为熟练的社会工程师选择的目标。攻击者可以轻易地从这些人手里得到表面上无害的信息，从而进一步获取更多敏感的公司信息。

攻击者选择新进员工的原因是他们不知道公司的特殊信息的价值或某种行为可能带来的后果，同样，他们也容易受到常用的社会工程学攻击的影响——动用了权威的呼叫者，似乎很友好很可爱，认识公司里受害者也认识的某个人，攻击者声称的很紧急的请求，或者其它能获得受害者好感（或认同感）的方法。

接下来有一些针对低层员工的攻击案例。

提供帮助的安全警卫

骗子希望能找到贪婪的人，因为他们是唯一可能陷入行骗游戏中的人。社会工程师（当他们瞄准了清洁队的成员或安全警卫之类的人时）希望能找到和善、友好、信任他人的人，他们是唯一最有可能提供帮助的人。这正是攻击者在下面的故事里所寻求的。

艾里特的观点

日期/时间：1998年二月的一个星期二，凌晨3:26

地点：新罕布什尔州纳舒厄Marchand微系统公司

艾里特斯泰雷（Elliot Staley）知道他不应该在上班时间离开岗位，但现在是半夜，我的老天爷，自从值班以来他一个人影都没看到，并且正好快到巡视的时间了，电话上的这个可怜的人似乎真的需要帮助，他们很乐意帮别人做一些事情。

比尔的故事

比尔快乐摇摆（Bill Goodrock）有一个简单的目标，一个从他十二岁以来就没变过的目标：二十四岁就退休，不用他的信托基金里的一分钱。

他告诉他的父亲，无情的、万能的银行家，他可以靠自己一个人成功。

然后过了两年，很明显他没有在二十四个月里成为杰出的商人，并且也没有成为精明的投资者，当然也没有发财。他曾经很想知道怎样持枪抢劫银行，但那只是小说中的素材——实在是太冒险了。所以他的白日梦就成了像瑞夫金那样——对银行实施电子抢劫。上一次比尔和家人一起去欧洲的时候，他打开过一个有100法郎的摩纳哥银行帐户，尽管里面只有100法郎，但他有一个

计划可以轻易地使这个数字达到七位，甚至是八位，如果运气好的话。

比尔的女朋友安玛丽在波士顿一家大银行的并购部门工作，有一天，她要参加一次漫长的会议，比尔只好在她的办公室里等她，出于好奇心，他把他的便携式电脑插入了会议室的以太网端口，是的！——他连上了他们的内部网络，从银行网络的内部……也就是说在公司防火墙的后面，这让他有了一个主意。

他的一个同班同学认识一个叫做朱莉亚的年轻女士，一个才华横溢的计算机科学博士，目前正在Marchand微系统实习。朱莉亚似乎是个不错的内部信息来源，比尔要开始施展自己的才华了。他们对她说他们正在写一个电影的剧本，她居然相信了，她认为和他们一起编故事很好玩，然后告诉他们怎样实现他们描述的那些事情，这个想法实在是太有才了，事实上，她还一直缠着他们，她也想出现在影片的致谢名单上。

他们警告说电影剧本的创意经常被偷，所以她发了誓绝不告诉任何人。

经过朱莉亚细心的指导之后，比尔要独自进入危险的部分了，他相信自己肯定能成功。

我下午打电话去的时候了解到晚上的安全主管是个叫以赛亚书亚当斯（Isaiah Adams）的人，于是我在那天晚上9：30打去电话，和安全部门的警卫交谈起来。我的故事显得很急促，听上去我还有些惊慌失措。“我的车子出毛病了，现在不能来公司，”我说，“我居然碰到了这样的事情，现在我很需要你的帮助，我想打给安全主管以赛亚书，但是他不在家，你能不能帮我一个忙？万分感谢！”

这家大型公司的每一个房间都有一个邮寄地址编码，所以我告诉他计算机实验室的编码并询问他是否知道在哪里，他说去那里要花一些时间，然后我说我会打到实验室的，很抱歉我使用了我能用的唯一的电话线路，我要用它来拨入网络尝试解决问题。

当他到达那里的时候，我打去电话告诉他哪里可以找到我感兴趣的那个控制台，上面标着“elmer”字样的主机——朱莉亚说这台主机是用于创建对外销售的操作系统正式版的。当他说他找到了的时候，我更加确定朱莉亚给我们提供了正确的信息，我的心扑通扑通直跳，我要他按几次回车，然后他说屏幕显示#号，这说明这台计算机已经用root用户（拥有所有系统权限的超级用户）登录了。他打字的时候要看着键盘，所以当我把要输入的下一个命令告诉他时，他费了好大力气才输入完成，非常谨慎：

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

最终他输入的很正确，现在我们有了一个名为fix的帐户，然

后我要他输入：

echo 'fix: :10300:0:0' 55 /etc/shadow

这是在设置密码，两个冒号之间什么都没有意味着密码为空，这两个命令把fix帐户用空密码添加到了密码文件中，这个帐户拥有和超级用户一样的权限。

下一步我让他输入了一个递归目录的命令，打印出一长串文件名列表，然后我要他把那张纸扯出来，带回警卫室，因为“等一下我可能会需要你从那上面为我读一些东西。”

最美妙的是他根本就不知道自己创建了一个新帐户，我让他把文件名的目录列表打印出来，因为我需要确认他之前输入的这些命令和他一起离开了计算机室，这样系统管理员或工作人员第二天早上就不会发现这里出现了一个安全漏洞。

现在我有了一个帐户，一个密码，和完整的权限，接近半夜的时候我拨入了主机，然后按照朱莉亚“给剧本”的指示，一眨眼的功夫我就进入了一个包含这家公司新版操作系统源代码的开发主机。

我上传了一个朱莉亚写的补丁，她说这修改了操作系统库中的一个程序，可以生成一个隐蔽的后门用于远程访问系统。

注释：

这里使用的后门并没有修改操作系统的登录程序，而是一个包含有登录程序使用的动态库的秘密入口。在常见的攻击中，电脑入侵者经常替换或修补登录程序自身，但是精明的系统管理员还是可以通过比较版本标记（就像CD一样）或其它方法察觉出来。

我小心地遵循着她写给我的指示，首先安装补丁，然后设法移除fix帐户并删去日志中的所有记录，这样就消除了我活动的痕迹，非常有效。

不久这家公司就开始把这个新的操作系统提供给他们的客户：全球的金融机构。他们送出的每一份拷贝都包含有我之前放入开发主机的后门，让我可以访问每一家升级了操作系统的银行和经济行的电脑系统。

术语：

补丁：修正一个可执行程序的一些代码。

当然，还没到休息的时候——还有一些事情要做。我还要获得每一家我想要“参观”的金融机构的内部网络访问权限，然后找出他们用来金融转账的电脑，在上面安装监控程序，了解他们是

如何操作的，确切的说是怎样转移资金的。

所有这些都可以远程进行，从有电脑地方，比如，白沙海滩。塔希提岛，我来了！

我回电给那个警卫，对他的帮助表示感谢，然后要他把那张打印出来的东西给扔了。

过程分析

那个安全警卫阅读过他的职责说明，即使是这样深思熟虑出来的说明也无法预测每一种可能出现的情况，没有人告诉他帮助一个他认为是公司员工的人在电脑上输入一些东西会伤害到公司。

有了警卫的帮助，他轻易地获得了一个重要系统（存储用于发布的产品）的访问权限，虽然实验室的门是锁着的，但警卫有所有门的钥匙，不是吗？

即使是本性诚实的员工（在这里，是候选博士和实习员工朱莉亚）有时也能被贿赂或被欺骗，无意中向社会工程师透漏出重要信息，比如目标计算机系统所在的位置——此次攻击成功的关键——他们何时发布软件的新版本，这很重要，因为如果过早的进行了改动，会大大增加被发现或失败的可能性，他们可以从一个干净的来源重建操作系统。

你让警卫把印出的资料带回警卫室并将其销毁了吗？这是很重要的一步，当电脑操作员第二天来上班时，攻击者可不希望他们在打印机终端上找到这该死的证据，或者在垃圾桶里发现它。给警卫一个似是而非的理由让他把印出的资料带走，避免冒险。

米特尼克语录

当计算机入侵者自己无法从物理上访问计算机系统或网络时，他会尝试利用别人帮他这样做。如果为了完成计划必须要进行物理访问，那么通过受害者代理要比亲自动手好得多，因为攻击者可不想有被察觉和被逮捕的风险。。

紧急更新

你可能认为技术支持人员十分清楚让外部人员访问公司网络的危险性，但是如果这个外部人员是一个聪明的社会工程师（伪装成了提供帮助的软件厂商），结果可能会出乎你的意料。

帮助电话

呼叫者想要知道谁负责这里的计算机，电话接线员帮他接通了技术支持人员，保罗阿赫恩（Paul Ahearn）。

呼叫者声称，“我是爱德华，来自SeerWare公司，你们的数据

库供应商。显然我们的一些客户没有收到我们的关于紧急更新的电子邮件，所以我们打电话给一些客户，作为质量监督检查是否已经装好了补丁，你安装了更新吗？”

保罗十分肯定地说，“我从没看到过类似的东西。”

爱德华说，“好的，这可能导致数据灾难性丢失，所以我们建议你尽快安装好补丁。”是的，这正是他想要做的，保罗说，“好的。”呼叫者回应说，“我们可以送给你包含补丁的磁带或CD，我想要告诉你的是，这真的很危险——有两家公司已经失去几天的数据了，所以你真的应该在收到之后马上进行安装，趁你的公司还没有发生那种情况之前。”

“我能从你们的网站上下载吗？”保罗问道。

“很快就可以了——技术团队正在努力当中，如果你愿意的话，我们可以让我们的客户支持中心远程帮你安装，我们可以拨号进入，也可以使用Telnet进行连接，如果你能支持的话。”

“我们不允许Telnet连接，特别是从因特网——这不安全，”保罗回答说。“如果你能用SSH的话，就没问题了。”他说，SSH是提供文件安全传输的产品名称。

“是的，我们有SSH。那么，IP地址是多少？”

保罗把IP地址告诉了他，并且当安德鲁问“我能用哪个用户名和密码”时，保罗也十分配合地说了出来。

过程分析

当然，那个电话也有可能真的是数据库厂商打来的，但那就不是这本书应该讲的了。

在这里，社会工程师首先让受害者担心数据有可能丢失，然后向他提供了一个直接了当的解决方案。

同样，当社会工程师选中的目标十分了解信息的价值时，他就要拿出非常可信非常有说服力的理由获得远程访问的权限，有时候他还需要催促一番，使受害者感到心烦意乱，让他在仔细思考这些请求之前就匆匆忙忙地同意了。

新来的女孩

在你的公司文件中有哪些信息可能是攻击者想要得到的？有时候可能是你认为根本就没必要保护的东西。

莎拉（Sarah）的电话

“人力资源部，我是莎拉。”

“你好，莎拉，停车场，我是乔治。你知道你用来进入停车场和电梯的门禁卡（译者注：与信用卡外观相似，内有编码数据）吗对，我们遇到了一个问题，需要重写最近十五天加入公司的所

有新员工的磁卡。”

“所以你需要他们的名字？”

“还有他们的电话号码。”

“我可以查看我们的新员工列表，到时候打给你吧，你的电话号码是？”

“73……啊，我现在有点事情，半个小时候我再打给你怎么样？”

“哦，好吧。”

当他再打回去的时候，她说：

“哦，是的，只有两个，一个是安娜莫托（Anna Myrtle），她是财政部的秘书，另一个是新来的副总，安德伍德先生。”

“电话号码是？”

“好的，安德伍德先生的号码是6973，安娜莫托的是2127。”

“嘿，你帮了我一个大忙，谢谢。”

安娜的电话

“财政部，我是安娜。”

“我很高兴有人这么晚了还在工作，听着，我是罗恩维特诺（Ron Vittaro），商务部的出版人。我不认为我们已经被介绍过了，欢迎来到我们公司。”

“噢，谢谢。”

“安娜，我现在在洛杉矶，我有一些事情，能占用你大概十分钟的时间吗？”

“当然，有什么可以帮忙的吗？”

“到我的办公室去，你知道我的办公室在哪里吗？”

“不知道。”

“好的，我的办公室在十五楼——1502室。过一会儿我会打电话到那里，如果你到了，就按一下电话上的转移键，这样来电就不会直接转到我的语音信箱。”

“好的，我这就去。”

十分钟后她到他的办公室取消了他的呼叫转移，然后等他的电话。他让她打开电脑，运行Internet Explorer，输入地址：www.geocities.com/ron-insen/manuscript.doc.exe。

出现了一个对话框，他告诉她点击打开。电脑开始下载这个文档，然后屏幕变成了空白。当她反应说好像出了点问题时，他的回答是，“噢，不，别再这样了，在网上下载东西的时候我经常遇到这个问题，我还以为已经解决了，那么，好吧，不要担心，我再试试其它方法。”然后他要她把他的电脑重启，好让他确认是否还会再出现这种情况，他告诉了她重新启动的操作步骤。

当电脑又一次毫无显示的时候，他对她的热心帮助表示了感

谢并挂上了电话，安娜回到财政部，继续她未完成的工作。

库尔特狄龙的故事

Millard-Fenton出版社对他们刚刚签约的新作家非常热情，财富500强公司的离任CEO，他要讲述一个迷人的故事。有人安排他和一个商务经理讨论相关事务，而这个商务经理不想让他知道出版合同的详细内容，于是他雇用了一个老朋友帮他找出他想要知道的东西。可惜的是，这个老朋友，并不是一个明智的选择。库尔特狄龙（Kurt Dillon）习惯于在他的调查中使用与众不同的方法，而这些方法并不完全符合道德。

库尔特在Geocities上用罗恩维特诺的名字申请了一个免费站点，然后上传了一个间谍程序，他把这个程序的文件名改为manuscript.doc.exe，这样看上去就是一个Word文档，而不会引起怀疑。事实上，这比库尔特预期的更有效：真正的维特诺从未更改过Windows操作系统的默认设置——“隐藏已知文件类型的扩展名”，因此实际显示的文件名为manuscript.doc。

他让一个女性朋友打电话给维特诺的秘书，按照狄龙的指示，她说：“我是多伦多终结者书店经理保罗斯帕多内（Paul Spadone）的执行助理，前阵子维特诺先生在一个书展上遇到了我的上司，他要他打电话给他商讨一个合作项目。斯帕多内先生有非常多的时间是在四处奔波，所以他说我应该弄清楚维特诺先生在办公室的时间。”

等到两个人核对好了时间表，这位女士就有了足够的信息提供给攻击者——一张维特诺先生在办公室的日程表，这意味着他同样知道了维特诺先生不在办公室的时间。不需要过多额外的交流就可以了解到维特诺的秘书会利用他不在的一段时间去滑雪，虽然时间不是很长，但两个人都不会在办公室，非常好。

术语

间谍程序：用于监控目标计算机活动的专业软件。一种形式是记录因特网购物者访问过的站点，这样在线广告就可以根据他们的上网习惯进行修改，另一种形式类似于监听，除了目标设备是计算机。这些软件监控用户的活动，包括密码、按键、Email、聊天记录、即时聊天、所有访问过的网站和显示屏图像。

无声安装：在计算机用户或操作员毫不知情的情况下安装软件程序的一种方法。

星期天他们按照预定计划打去电话进行确认，然后被一个接待员告知“维特诺先生不在办公室，他的秘书也不在，最近几天都别指望他们会在。”

他的初次尝试非常成功地使一个新进员工加入到了他的计划中，她毫不犹豫地帮他下载了一个“manuscript”（原稿）文件，而事实上这个文件是一个流行的商业间谍程序，攻击者把它改成了无声安装，通过这种方法，安装程序就不会被任何杀毒软件发现。因为一些奇怪的理由，杀毒软件厂商销售的产品并不能识别商业化的间谍程序。

当这位年轻女士在维特诺的计算机上运行了那个程序之后，库尔特马上回到了Geocities站点上，他把那个doc.exe文件替换成了一个他在网上找到的书籍原稿，以防有人无意中发现了这个骗局并回到该站点进行调查，他们唯一能找到的是一份无用的、业余的、不适合出版的书籍原稿。

一旦程序安装完成并重新启动了计算机，设置马上就会生效。罗恩维特诺将在几天后回到这里开始工作，间谍程序也将开始记录他的计算机上的所有键入，包括所有寄出的Email和那时他的屏幕上显示的图像，所有这些都将被定期发送到一个乌克兰的免费邮箱上。

在维特诺返回数天后，库尔特的邮箱里已经堆满了收集的日志文件，不久之后他在一封秘密的电子邮件里发现了Millard-Fenton出版社与作家达成协议的底线，有了这些信息，就可以通过代理和出版社商讨比原来更好的合同条款，而不会有失去合作机会的风险，当然，这也意味着需要更多的代理费。

过程分析

在这个骗局中，攻击者之所以能成功很大程度上是因为他选择了一个新进员工作为他的代理，多亏了她自愿的合作成为了团队的成员，既不了解公司和它的员工，也不清楚哪些是可以抵挡攻击的好的安全习惯。

因为库尔特在和安娜的谈话中伪装成了商务部的副部长，他知道她不太可能会怀疑他的身份，相反的，她可能认为帮助一个副部长对自己很有好处。

接着他引导安娜安装了一个表面上无害的间谍程序，安娜并不知道她的行为让一个攻击者获得了能影响公司利益的重要信息的访问权限。

为什么他要选择把这个副主管的日志文件发到一个乌克兰的邮箱帐户里？因为距离越远攻击者被追踪或抓捕的可能性就越低。当警察把目光集中在并不显著的的因特网入侵上时，这个国家就不会受到攻击者的青睐。因此，使用国外的邮箱可以大大减少和美国执法部门打交道的机会，这很吸引人。

预防措施

社会工程师永远喜欢不怀疑他的请求的人，这不仅使他的工作变得容易，而且也使风险变得更低——正如这一章中的故事所讲的那样。

米特尼克语录

寻求同事或下级的帮助是一件很普通的事情，社会工程师知道怎样利用人们的天性获得帮助并使其成为团队的成员。攻击者利用人们的这种特点引导员工的行为以达到他的目标，了解这一简单的概念非常重要，这样在另一个人试图操纵你的时候你就更有可能发现。

欺骗不知情的人

我之前强调的是需要对员工进行充分的培训，使他们不会被陌生人说服去做某些事情， 所有员工同样需要了解按照请求在另一个人的计算机上执行任何操作都是很危险的，公司的政策应当禁止这些行为，除非得到一名指定的管理人员的批准。允许的情况包括：

当发出请求的是一个你非常熟悉的人，两个人面对面或者你通过电话确认了呼叫者的声音时。

当你通过严格的程序核实了请求者的身份时。

当行动得到一名主管或其他熟悉请求者的权威人士的批准时。

必须培训员工不去帮助不是亲自认识的人，即使那个人声称自己是经理主管人员。一旦安全政策方面的审核开始实施，管理层就必须让员工们遵守这些规定，即使这意味着员工可以质疑要求他们绕过安全规定的主管人员。

每家公司还需要有自己的政策和程序引导员工响应针对电脑或电脑相关设备的任何行动。在这个关于出版社的故事中，社会工程师有针对性的选择了一个没有接受过信息安全策略与程序培训的新员工。为防止这类攻击，所有员工都必须遵守这样一个简单的规则：不要在任何计算机系统上执行陌生人请求的操作，就这一点。

记住，任何能直接或间接接触到一台计算机（或一部与计算机相关的设备）的员工都很容易被攻击者操控成为实施一些恶意行为的代理。

员工们（尤其是IT员工）需要知道让外部人员进入他们的计算机网络就像是把你的银行帐户交给一个电话销售员或把你的电

话卡号码交给一个监狱中的陌生人。员工们必须谨慎考虑那些能导致敏感信息泄露或危及公司计算机系统安全的请求。

IT员工也必须提防伪装成供应商的未知呼叫者。通常，公司应当考虑为每一个技术供应商指定具体的联系人员，如果实施了这一策略，其他员工就不会响应供应商索取资料或更改任何电话或电脑设备的请求。这样，指定的员工就会很熟悉打电话或前来拜访的供应商, 减小了被骗的可能性。如果一个和公司没有合同的供应商打来电话，也应当引起注意。

公司中的的每个人都必须了解信息安全威胁与攻击。注意，安全警卫等需要的不仅仅是安全培训，还应当包括信息安全培训，因为安全警卫经常要接触公司的设施，所以他们必须要能够识别各类针对他们的社会工程学攻击。

当心间谍程序

商业间谍程序曾经被许多家长用来监控他们孩子的网络行为，而对于公司的老板而言，他们需要找出那些不认真工作，只知道上网冲浪的员工，更重要的是找出那些潜在的信息窃贼或商业间谍。开发商推出间谍软件似乎旨在保护儿童，但事实上，他们真正的市场是那些想要暗中监视别人的人。如今，间谍软件之所以存在在很大程度上是因为人们想要知道他们的配偶或其他重要人物是否在骗他们。

前不久我开始写这本书中的间谍故事的时候，帮我收电子邮件的人（因为我被禁止上网）发现了一封宣传一系列间谍程序的广告邮件，其中一段是这样说的：

热门！必须拥有：

这一强大的监控程序秘密捕获所有的按键、时间与所有活动窗口的标题到一个文本文档，同时隐藏在后台运行。日志文件可加密并自动发送到指定邮箱地址，或仅存储在硬盘上。程序受密码保护并可在CTRL＋ALT＋DEL菜单中隐藏。可用它来监控输入的网址、聊天记录、电子邮件和许多其它东西（甚至是密码）。

在任何PC上后台安装并把日志发给自己！

杀毒软件的缺陷？

杀毒软件不能查出商业间谍程序，从而将其判定为非恶意软件，即使它的用途是监控他人。如此一来电脑就相当于一部被忽视的窃听器，在任何时候我们每个人都有被非法监控的危险。当然，杀毒软件厂商可能认为，间谍程序可以用于合法目的，因此不应当视为恶意软件。但是由黑客团体免费发布（或当成安全相关程序出售）的某些工具却会被视为恶意代码，我至今都不明白为什么会有这种双重标准。

同一封邮件中的另一段则声称它可以捕捉用户的电脑屏幕图像，就像是一台放在他肩膀上的摄像机。其中部分软件产品甚至不需要亲自接触受害人的电脑，只要远程安装并配置好应用程序，你就马上拥有了一部电脑窃听器！FBI（联邦调查局）肯定很喜欢这种技术。

由于间谍程序的广泛使用，你的企业需要建立双层防护。你应当在所有工作站上安装间谍程序检测软件，如SpyCop （网址：www.spycop.com），你还应当要求员工进行定期扫描。此外，你还必须培训员工提防下载程序或打开电子邮件附件之类的可以安装恶意程序的骗局。

除了防范间谍程序的安装（当员工因为茶会、午餐或会议离开办公桌时）以外，还应当规定所有员工在离开时必须使用屏幕保护密码或类似的方法锁定他们的计算机系统，这能大大降低员工的计算机被非法访问的可能性。即使混入某个人的房间或办公室也不能访问他们的任何文件，阅读他们的电子邮件或安装间谍程序（或其他恶意软件）。使用屏幕保护密码需要的资源几乎为零，却能很好地保护员工的工作站，在这种情况下进行成本效益分析应该是很容易的事情。

# 第十三章 聪明的骗局

现在你已经知道了，当接到陌生人请求敏感信息（或其它对攻击者有用的东西）的来电时，接电话的人必须被培训询问呼叫者的电话号码，然后打过去核实这个人的身份是否和他声称的一样——例如，一名公司员工，一名商业伙伴员工，或者一名供应商技术支持代表。

甚至当一家公司明确规定员工必须小心核实呼叫者的身份时，经验丰富的攻击者仍然可以利用许多骗局使受害人相信他们是他们声称的人，即使是安全意识较高的员工也会被下面所述的方法所骗。

骗人的来电显示

任何用手机接过电话的人都曾看到过来电显示——显示屏上呼叫者的电话号码。在商业环境下，员工只要看一眼便能知道打来的电话是公司同事还是外部人员。

很多年前，一些雄心壮志的电话盗打者就已经用上了来电显示功能，那时电话公司甚至还没有向公众开放这一服务，有一段时间他们吓坏了不少人，接电话的时候总是在对方还没来得及说话之前就喊出他们的名字。

当你养成了看来电显示的习惯时，你认为它是安全的并以此判断呼叫者的身份——这正是攻击者想要的。

琳达的电话

日期/时间：7月23日，星期二，下午3:12

地点：星级漫游航空公司财政部办公室

当琳达希尔（Linda Hill）的电话响起的时候她正在为她的老板书写备忘录，她看了一眼来电显示，发现是一个叫维克托马丁（Victor Martin）的人从公司在纽约的办公室打来的——她不认识这人。

她本来想把电话转到语音信箱，这样她就不会中断写备忘录的思路，但好奇心还是占了上风，她拿起了电话，然后对方自我介绍说他是产品推广部的员工，正在为CEO整理一些材料，“他正在赶往波士顿和我们的一些银行家开会，他需要本季度的财务报表，”他说，“另外，他还需要Apache项目的财政预算。”维克多提到了公司春季主打产品代号。

她问他要电子邮件地址，但是他说他现在无法接收电子邮件，技术人员正在想办法解决，能否传真过来？她说也可以，然后他把他的内部传真号给了她。

几分钟后她发出了传真。

但维克多并不在产品推广部工作，事实上，他甚至不是这家公司的员工。

杰克的故事

杰克道金斯很年轻的时候就开始了他的职业生涯——在纽约人体育场、拥挤的地铁月台和夜间聚集着游人的泰唔士广场行窃。他可以从一个人的手腕上取下手表而不被发现，可见他动作之敏捷手法之高超。但在他充满烦恼的少年时期，他却因失手而被抓了。在少管所里，杰克学到了一个新职业，被抓住的可能性非常之低。

他当前的任务是获得一家公司的季度损益表与现金流量信息，要在这些数据被提交到美国证券交易委员会( SEC )并公布之前。他的客户是一个不愿意解释为什么需要这些信息的牙医，这个人的小心翼翼在杰克看来十分有趣，他之前的推测是——这家伙可能赌博赢了钱，要么就是有一个一直没被他的妻子发现的有钱的女朋友，或者也有可能是向他的妻子吹嘘了自己在股票市场的英明神武，总之现在他已经失去了所有的管束，只想进行一大笔投资，在这家公司公布他们的季度财务报表之前，预测他们的股票价格将如何变化。

人们惊讶地发现，细心的社会工程师可以迅速地应对从未遇到过的情况。当杰克从牙医那里回到家的时候，他已经想好了一个计划。他的一个朋友查尔斯贝茨（Charles Bates）在Panda进出口公司工作，这家公司有自己的电话交换机或PBX（译者注：专用分组交换机）。

在了解电话系统的人熟悉的术语中，PBX连接着数字电话服务T1，并被设置为初始速率接口ISDN（综合服务数字网络）或PRI ISDN，这意味着从Panda打出的每一个电话都会通过一个数据频道发送呼叫处理信息到电话公司的交换机：这些信息包括将转到（除非被锁定了）对方来电显示上的主叫号码。

杰克的这个朋友知道怎样修改交换机让接到电话的人在来电显示上看到伪造的号码，而事实上电话是从Panda办公室打来的。这种骗局之所以有效，是因为当地电话公司懒得去验证客户的呼叫号码是不是实际上付钱的那个号码。

杰克道金斯需要的只是使用这种电话服务，幸运的是他的朋友与合作伙伴查尔斯贝茨总是乐于伸出援助之手，而只收取象征性的费用。在这里，杰克和查尔斯临时修改了电话交换机的设置，让Panda公司的一条指定电话线路使用维克托马丁的内部电话号码，这样电话看上去就是从星际漫游航空公司打出的了。

你的来电显示不会出错，很多人都这样想，在这里，琳达愉快地把资料传真给了她认为是产品推广部员工的人。

当杰克挂上电话时，查尔斯又把交换机的设置给改了回来。

过程分析

一些公司不想让客户或供应商知道他们员工的电话号码。比如，福特公司规定，从他们的客户支持中心打来的电话应当显示800号码和“福特支持”字样，而不是每一个客户支持代表真实的电话号码。微软公司则让员工自己选择是否把电话号码告诉别人，并不是每一个接到他们电话的人都能看到来电显示并找出他们的位置。通过这种方法公司便能保持内部号码的隐匿性。

但是修改交换机设置对于一些人而言是在是太简单了，比如，恶作剧爱好者、收账单的人、电话销售员，当然，还有社会工程师。

变奏：美国总统来电

作为洛杉矶KFI谈话节目"互联网黑暗面"的客串主持人，我认识电台的节目总监大卫，他是我见过的最勤奋最负责的人，你很难电话联系到他，因为他实在是太忙了。他不接任何电话，除非来电显示上出现了他必须谈话的人。

当我打电话给他时候，因为我的手机出了问题，他不知道是谁的电话所以没有接，而让它转到了语音信箱，这让我觉得很失败。

我和一个老朋友详细地讨论了这件事，他创办了一家专门为高科技公司提供办公室的房地产公司。我们一起制定了一个计划，他可以使用他们公司的子午线电话交换机，也就是说他可以修改主叫号码，就像刚才的故事描述的那样。每当我需要联系节目总监但又打不通电话时，我就请我的朋友帮忙修改来电显示上的号码，有时候我想让电话看上去是大卫的办公室助理打来的，有时候则是电台的控股公司。

但我最喜欢的还是把它改成大卫自己家的电话号码，他总是会接，因为他信任这个人。当他拿起电话并发现我再一次和他开了个玩笑时，他永远都是那么幽默。当然，他会在线足够长的时间解决我的所有问题。

当我在阿特响铃秀上证明这一小小的骗局时，我让我的来电显示出现了FBI洛杉矶总部的名字和号码。阿特对整件事情非常震惊，他警告我说这是违法的，但我告诉他这是完全合法的，只要不用来诈骗。在那次节目之后我收到了几百封电子邮件，他们想知道我是怎么做到的，现在你知道了。

这对社会工程师而言是获得信任的绝佳工具，例如，在社会工程学攻击的调查阶段，只要目标有来电显示，攻击者就可以让他或她的电话看上去是从可信的公司或员工打来的，收账单的人

也可以让他或她的电话看上去是从你的办公场所打来的。

想一下这意味着什么，计算机入侵者可以在家里打电话给你，声称自己是你公司的IT部门员工，然后说服务器崩溃了，他需要你的密码来恢复你的文件；或者电话上出现了你的银行或证券交易所的名字，一个声音甜美的女孩想确认一下你的账户号码和你妈妈的婚前姓，另外，因为系统出了一些问题，她还需要核对你的ATM　PIN码；股票市场的证券欺诈经营者可以让他们的电话看上去是来自美林证券公司或花旗银行；某个想盗窃你身份的人可以从移民局打来电话，让你告诉他你的签证卡号；一个嫉恨你的家伙可以打来电话声称自己来自IRS（译者注：美国国税局）或FBI。

如果你通过一个电话系统连接上了一个初始速率接口（PRI），那么再加上一点点从系统供应商的网站上学到的编程知识，你就可以用这种方法和你的朋友开玩笑。认识的某个人有强烈的政治愿望？你可以把呼叫号码改成202-456-1414，这样他的来电显示就会出现“白宫”的名字。

他会认为自己接到了总统的电话！

这些故事要表达的意思很简单：不能信任来电显示，除非已经确认是内部号码。无论是在工作中还是在家里，每个人都需要知道这种骗局并意识到来电显示上出现的名字和电话号码是无法验证身份的。

米特尼克语录

下一次当你接到电话时，如果来电显示上的是你亲爱的老妈，谁知道啊——她可能是个年轻可爱的社会工程师。

无形的员工

雪莉卡特拉斯（Shirley Cutlass）找到了一个新的令人激动的赚钱方法，告别长时间的既辛苦又乏味的工作，她加入到上百个侵淫此道数十年的行骗艺术家当中，成了一名身份窃贼。

现在她的目标是获取一家信用卡公司客户服务部门的机密信息，在常规的准备之后，她打到目标公司，告诉接线员她想要连线电信部门，然后她对电信部门的人说她想和语音信箱的管理员通话。

利用她之前搜集的信息，她自称为克里夫兰办公室的诺玛托德（Norma Todd），现在你应该很熟悉这个骗局，她说她将在一周后前往公司总部，她需要一个这里的语音信箱，这样她就不用打长途电话查看她的语音信息。他说他会在办好之后回电话给她，因为会有一些她需要的信息。

她用迷人的声音说，“我在去开会路上，我能在一小时后打给你吗？”

当她打回去的时候，他说已经设置好了，然后是一些必要的信息——她的分机号和临时密码。他问她是否知道怎样更改语音信箱的密码，虽然她知道的并不比他少，但她还是让他讲解了一遍操作步骤。

“顺便问一句，”她说，“从我的旅馆，要打哪个号码才能查看我的信息？”他给了她那个号码。

然后雪莉打了进去，更改了密码并录入了新的问候语。

雪莉的入侵

到目前为止一切都很简单，现在她准备施展欺骗的艺术了。

她打电话到目标公司的客户服务部门，“克里夫兰办公室人力资源部，”她说，然后变化了一下这个耳熟能详的借口，“技术支持人员正在修理我的电脑，我需要你帮忙查找这些信息。”接着她提供了一些她想要窃取身份的人的名字和生日，然后她列出了她想要的信息：地址、母亲的婚前姓、卡号、信贷限额、可用信用、支付历史。“按这个号码打给我，”她给出了语音信箱管理员为她设置的内部分机号，“如果我不在的话，只要在我的语音信箱里留言就可以了。”

她一早上都在忙其它事情，然后在下午查看了她的语音信箱，她想要的信息都在。在挂电话之前，雪莉清除了问候语：如果不小心的话会留下她的声音记录。

身份盗窃是美国增长率最高的犯罪形式，“在”新世纪的犯罪中，总会有下一个受害者。雪莉用她刚刚得到的信用卡与身份信息开始了刷卡消费。

过程分析

在这个骗局中，攻击者首先让语音信箱管理员相信她是公司的一名员工，这样他就帮她设置了一个临时的语音信箱。如果他进一步进行了核实，他会发现她给出的名字和电话号码可以和公司的员工数据库列表匹配。

接下来的事情很简单了，以电脑故障为由，请求需要的信息，并要求在语音信箱中留言。有什么能阻止员工和同事分享信息？只要看到雪莉提供的内部分机号，就没有任何怀疑的理由。

米特尼克语录

试着偶尔打到你自己的语音信箱，如果你听到问候语不是你的声音，你可能已经遇到你的第一个社会工程师。

提供帮助的秘书

骇客（Cracker）罗伯特乔迪（Robert Jorday）经常入侵一家环球公司的网络，鲁道夫海运公司。最终这家公司发现有人入侵了他们的终端服务器，通过这台服务器用户可以连接到公司的任意一台计算机。为了维护公司网络，这家公司决定在每一台终端服务器上添加一道拨号密码。

罗伯特伪装成法务部的律师打电话到网络操作中心说他无法连接网络，接电话的网络管理员解释说出台了新的安全措施，所有的拨号访问用户都必须从他们的经理那里获得一个每月密码。罗伯特想知道经理是怎样得到这个每月密码，得到的回答是，下个月的密码会写入备忘录，然后通过办公室邮寄给每一位公司经理。

这让事情变得很简单，罗伯特稍微调查了一下，然后在月初打电话到这家公司，连线了一位经理的秘书，她说自己叫珍妮特。他说，“嗨，珍妮特，我是研发部的兰迪古德斯丁（Randy Goldstein），我知道备忘录里有从公司外部登录终端服务器的每月密码，但是我怎么也找不到，你能从你的备忘录找到它吗？”

是的，她说，她找到了。

他问她是否可以把它传真过来，然后她同意了，他给了她一个前台接待员（在这家公司的另一栋大楼里）的传真号码，他已经安排好了一切，包括把密码传真转发出去。在这里，罗伯特转发传真的方法有点与众不同，他给了接待员一个在线传真服务的号码，如果他们收到了传真，系统会自动转发到客户的电子邮箱地址。

新密码将被发送到一个Email秘密传送点，罗伯特选择了中国的免费电子邮箱。他知道如果这个传真被跟踪了，调查者可以与中国官方合作把他给揪出来，但是，他们也许并不想被这种小事打扰。最棒的是，他甚至没见过那台传真机。

米特尼克语录

人们总是乐于帮助一名熟练的社会工程师，接收一份传真并把它转发到另一个地方似乎是无害的，让一个接待员（或其他人）答应帮忙实在是太简单了。当有人向你请求一些信息时，如果你不认识他或无法核实他的身份，只要拒绝就可以了。

交通法庭

或许每一个接到过超速罚单的人都做过关于逃避处罚的白人梦，不去交通法规学习班，只支付罚款，或碰碰运气设法让法官

相信警车计速器（或雷达测速仪）出了一些技术问题。利用系统的漏洞，这个美好的愿望即将实现。

骗局

虽然我不建议你使用这种方法逃避罚单（有句话说的好，请勿轻易尝试），但这仍然是一个很好的社会工程学案例。

我们就叫这个交通违规者保罗杜里（Paul Durea）好了。

第一步

“霍伦贝克区，洛杉矶警察局（LAPD）。”

“你好，我想和传票管理员谈话。”

“我就是。”

“好的，我是米查姆和塔尔波特的代理律师，我需要在法庭上传唤一名警官。”

“没问题，你要传唤谁？”

“肯德尔警官是你们区的吗？”

“他的编号是？”

“21349。”

“是的，你什么时候需要他？”

“下个月的某个时候，我还需要传唤其他几个证人才能确定开庭时间，肯德尔警官下个月有哪些安排？”

“让我来看看……20号到30号是他的假期，他将在8号和16号参加培训。”

“谢谢，我需要的就是这些，开庭日期定下来我会再打给你的。”

地方法院，办事员前台

保罗：“我想要确定一下这张交通告票的开庭日期。”

办事员：“好的，我可以帮你安排在下个月的26号。”

“好，我想要安排一次传唤。”

“你想为交通告票传唤某个人？”

“是的。”

“好吧，我们可以把传唤设在明天上午或者下午，你想设在什么时候？”

“下午。”

“传唤设在明天下午1:30，在第六法庭。”

“谢谢，我会来的。”

地方法院，第六法庭

日期：星期四，下午1:45

办事员："杜里先生，请靠近长椅。"

法官："杜里先生，你了解你的权利了吗？"

保罗："是的，法官大人。"

法官："你愿意参加交通法规学习班的培训吗？你的案子将在你成功完成8小时的课程后取消，我查看了你的档案，你目前符合标准。"

保罗："不，法官大人。我恳请审判此案。还有一件事，法官大人，我要出国一段时间，只在8号和9号有空，能不能把我的案子的审判放在其中一天？我明天就要到欧洲进行商务旅行，我将在四周后回来。"

法官："非常好，审判设在六月八号，上午8:30，第四法庭。"

保罗："谢谢你，法官大人。"

地方法院，第四法庭

八号那一天，保罗很早就到了法院。当法官进来的时候，办事员给了他一张未出庭的警官列表，法官召集了所有被告，包括保罗，然后告诉他们他们的案子被取消了。

过程分析

当警官开罚单的时候，他会把他的名字和他的证件号码写在上面（或者其它可以联系他的私人号码），找到他工作的地方简直是小菜一碟。只要打个电话到号码服务台，查询一下写在传票上的执法机构名（公路巡逻局、县警察局、或者其它），事情就成功了一半，接着和那个机构取得联系，他们能提供给呼叫者传票管理员的电话号码。

执法部门的官员经常被法院传唤出庭作证：这是他们的职责之一。当检察官或辩护律师需要一名警官出庭作证时，如果他知道系统是怎样运转的，他就会首先确认这名警官是否有时间出庭。这很容易办到：只要打个电话给那里的传票管理员就可以了。

在谈话中，律师通常会询问那名警官在某月某日是否时间，为了实现这个骗局，保罗稍微变通了一下：他用一个似是而非的理由获知了那名警官无法出庭的时间。

当保罗第一次到法院去的时候，他为什么不直接告诉法院办事员他想安排在哪一天？答案很简单——我个人认为，大多数地方的交通法院办事员不允许让公众成员选择开庭日期，如果办事员提出的日期当事人无法接受，她会提供一个折中的选择，但是她会做出很大的让步。另一方面，想要获得额外的传讯时间的人可能会更走运一些，保罗知道他可以申请传讯，并且法官通常会

为传讯安排指定的日期。他请求在那名警官参加培训的那一天开庭，要知道在这种情况下，警员培训比出庭作证要重要得多。

米特尼克语录

人类的思想是一种神奇的产物，比如人们在脑海里设计骗局得到他们要想的东西或者脱离险境。你可以在公共与私营部门中利用同样的创造力与想像力保护信息与计算机系统的安全。所以，各位，当你们制定你们公司的安全策略的时候——要打破常规去思考问题。

在交通法院，如果传唤的警官没有出现——案子就会被取消，没有罚款，不用去交通学校，没有分数，最棒的是，不会留下任何交通肇事的记录！

我猜会有一些警务人员、法院办事员、检察官和类似的人读到这个故事会摇摇头，因为他们知道这种骗局是可行的，但他们只是摇摇头而已，我敢打赌不会有任何改变。就像电影《通天神偷》（1992年）中科斯莫说的那样，“一切只和零与一有关”——意思是，最终，所有的东西都将归结为信息。

只要执法机构愿意把一名警官的日程表提供给任何一个打电话来的人，人们躲避交通罚单的能力就会一直存在下去。聪明的社会工程师可以利用它来获取你不想让他们知道的信息，在你的公司或机构的程序中有类似的缺口吗？

萨曼塔的报复

萨曼塔格雷森生气了。

她一直在为她的大学商学位而努力，为此她还申请了一大笔助学贷款，因为她总是听到别人说，大学学位能让你成就一番事业，大学学位能让你赚到很多很多的钱。然后她毕业了，却发现自己连一份合适的工作都找不到。

收到蓝贝克制造公司的聘用协议着实让她高兴了好一阵子，虽然这份秘书工作对她而言实在是大材小用，但卡特莱特先生说他们很欣赏她，并承诺在下一个非行政职位空缺时将她纳入候选人中。

两个月后，她听说卡特莱特先生的一个产品采购经理离职了，那天晚上她很久都没有睡，想象着自己在五楼办公室出席会议并参与公司决策的样子。

第二天一大早她就遇上了卡特莱特先生，他说他们觉得在她胜任这一职位之前，她还需要学习更多的行业知识，然后他们从公司外面雇用了一个外行人，一个比她差多了的外行人。

她很快就明白了：这家公司有很多女职员，但她们清一色的

都是秘书，他们不会给她一份经理工作，永远也不会。

报复

她花了差不多一个星期才想好怎样报复他们。大概一个月前的产品发布会上，有一家商业杂志的记者想要采访她，几周后那个人打来电话说，希望她能提供一些Cobra 273的未公开信息，作为回报，他会送花给她，并且如果这些信息很有吸引力，他会专门从芝加哥跑来约她吃饭。

她每天会有一段时间待在乔汉森先生的办公室里，所以当年轻的乔汉森先生登录公司网络的时候，她站在后面看得一清二楚（有时候这也称为肩窥），他输入的密码是“marty63”。

她的计划已经开始实施了。她记得有一份备忘录是在她来公司后不久分发的，她在其中找到了一份复印件并仿照原始版本打印了一份新的，内容如下：

TO：C. 比尔顿，IT部

FROM：L. 卡特莱特，开发部

马丁乔汉森将转到我部门的专业研究小组工作，因此我授权他访问开发组使用的服务器，乔汉森先生的安全配置将更新为产品开发者权限。

路易斯卡特莱特

术语

肩窥：通过监视用户输入，窃取密码或其它用户信息的行为。

当大部分人都出去吃午餐的时候，她把卡特莱特先生的签名从最初的备忘录上剪切下来，粘贴到她的版本上面，并在四周涂上修正液。她把成果复印了一份，然后再复印了一份复印件，你几乎看不到签名四周的痕迹。最后她在卡特莱特先生办公室附近的传真机上把它发送了出去。

三天后，等到所有人都离开了公司，她走进乔汉森的办公室，尝试用的他的用户名和密码（marry63）登录网络，结果成功了。

只用了几分钟她就找到了Cobra 273的产品规格文件并将其下载到了Zip磁盘上。

当她在凉爽的夜间像风一般走入停车场的时候，那张磁盘正平平安安地待在她的钱包里，等待着和那名记者的见面。

过程分析

一个不满的员工，一次文件搜寻与快速剪切粘贴-修正液操作，少量有创意的复印与一份传真，然后，瞧！——她得到了机密的商业产品技术规格书。

几天以后，一家商业杂志的新闻记者独家报导了一个热门新产品的技术规格书和产品销售计划，这些都在产品发布之前几个月出现在了该杂志的所有订阅者手中，竞争对手将有几个月的时间抢先开发同类产品并在他们的广告活动中做好准备影响Cobra 273的发售。

当然，这家杂志绝不会透漏他们的消息来源。

防范措施

当被请求任何有益于竞争对手的贵重、敏感或关键信息时，员工们必须了解通过来电显示验证外部人员的身份是不被允许的，必须要有一些其它的验证方法，比如与此人的主管联系，确认这些请求是合法的，用户已被授权接收这些信息。

各公司必须自行控制验证程序中安全与效率的平衡。哪些安全措施应当被优先考虑？员工们会不会抵制这些安全措施？甚至绕过它们以完成他们的工作任务？员工们了解为什么安全对公司和他们自己都如此重要吗？这些问题的回答将帮助建立基于企业文化和商业需求的安全策略。

大部分人难免会认为这些安全措施妨碍到了他们的工作，连绕过它们都是在浪费时间。可以通过宣传和教育，鼓励员工们把安全工作当成他们的日常职责。

尽管不能用来电显示验证外部呼叫者的身份，但是另一种叫做自动号码识别（ANI）的服务却可以。当一家公司开通了免付费电话（由公司支付呼入费用）时，这种服务可以准确地识别呼叫者。与来电显示不同的是，电话公司交换机不会接受客户发送过来的呼叫号码，ANI传输的号码是分配给呼叫用户的付费号码。

另外，一些调制解调器厂商把来电显示功能添加到了他们的产品里，为保护企业网络而设定了只接受指定电话号码的远程访问。调制解调器的来电显示功能可以在安全级别较低的环境下作为身份验证的手段，但是，众所周知，伪造来电显示对于计算机入侵者而言并不是一件难事，因此在安全级别较高的情况下不能据此判断呼叫者的身份或位置。

在身份盗窃的案例中，管理员在企业电话系统上为入侵者创建了一个语音信箱，为了防止此类事件的发生，企业应当规定所有的电话系统、语音信箱和所有的企业目录（不管是印刷的还是在线的）在被使用时必须提出书面请求，形式固定，员工经理应当在这份请求上签字，然后交语音信箱管理员核实。

企业安全策略应当规定，在创建新的计算机账户或增加账户

权限时，必须向系统管理员或他（或她）的指定负责人核实该请求，可以在纸质或在线公司目录上找到相应的电话号码。如果你们公司使用经过数字签名的安全电子邮件，这种折中的验证方法也可以接受。

记住，每一个员工（不管他是否能访问公司的计算机系统）都有被社会工程师利用的可能性。每个人都必须接受安全知识培训。所有的行政助理、接待员、电话接线员和安全警卫都必须要熟知各类社会工程学攻击（大多数都是针对他们的），这样他们才能更好地防范这些攻击。

# 第十四章 商业间谍

针对政府、企业和大学机构的信息安全威胁已经很好地得到了介绍，几乎每一天都会有媒体报导新的计算机病毒、拒绝服务式攻击、电子商务网站的信用卡信息盗窃案。

我们经常读到关于商业间谍的新闻，比如，Borland指责Symantec盗窃商业机密，Cadence设计规划公司控诉竞争对手盗窃其产品源代码，许多商业人士认为在他们公司绝不会发生这种事情，但是，这种事情每天都在发生。

## 计划变更

下面故事中的骗局或许已经被实现过很多次了，虽然这很像是好莱坞电影（比如《The　Insider》）里的情节或者约翰格雷森姆的法律惊险小说。

## 集体诉讼

假设有一场针对Pharmomedic制药公司的集体诉讼，该诉讼声称他们发现该公司的一种非常受欢迎的药物具有破坏性的副作用，这种副作用将在病人服药多年以后显露出来，该诉讼声称他们是从一系列的调查研究中得出这一结论的，但是这些证据被压下不用，并且没有在规定的时间内转交给FDA（食品及药物管理局）。

威廉比利钱尼（William　"Billy"　Chaney），处理此案的纽约律师行代理律师，得到了两个Pharmomedic医生的证词，但是两人全都退休了并且没有任何档案或文件，所以不能作为令人信服的证人。比利知道自己现在处于弱势，除非他能得到其中一份报告或者内部备忘录（或公司高层之间的通讯）的副本，否则他的整个案子都将崩溃。

因此他选择了和一家公司再次合作：安德雷森父子私人调查公司。比利不知道彼得和他的人是怎样获得这些资料的，他也不想知道，他只知道彼得安德雷森（Peter　Andreeson）是一个好侦探。

至于安德雷森，他把像这样的任务称为黑袋子秘密调查，第一条规则就是让雇用他的律师事务所和公司不知道他是怎样获得这些信息的，所以他们总是解释得模模糊糊似是而非。如果有人愿意自找麻烦的话，越难的任务他所收取的费用越高，他认为这值得冒险，除此之外，他还能从欺骗聪明人的过程中找到个人满足感。

如果钱尼希望他找到的那些文件确实存在并且没有被销毁，他们也许会把它放在存放文件的某个地方，但是要从堆积如山的

文件中把它们找出来无疑是一项艰巨的任务。另一方面，假设他们已经把文件的副本交给了他们自己的律师事务所（詹金斯与派屈），如果辩护律师知道这些文件的存在并且不把它们转交到取证程序，那他们就违反了律师的职业道德并触犯了法律，在彼得看来，这制造了许多可攻击的对象。

彼得的攻击

彼得让他的人着手调查，几天后他弄清了詹金斯与派屈律师事务所存放异地备份的位置，他还了解到存储公司有一张律师事务所授权提取磁带的人员名单，名单的上的每个人都有各自的密码。彼得派了两个人进行这一次的黑袋子秘密调查。

他们用从网上（www.southord.com）买来的开锁工具开锁，几分钟后就溜进了存储公司的办公室（大概凌晨3点），其中一人打开一台PC机，屏幕上出现了Windows 98的图标，他们笑了，这简直就是小菜一碟，Windows 98没有任何形式的身份认证程序。稍加搜索之后，他们找到了含有授权名单的Microsoft Access数据库。他们在詹金斯与派屈律师事务所的授权名单上添加了一个伪造的名字，其中一人早就准备好了匹配的驾驶执照，当然也是假的。他们能闯入带锁的存储室并找到他们客户想要的磁带吗？当然能——但是，这家公司所有的客户（包括律师事务所）都会收到一张受损通知，这样一来攻击者就失去了应有的优势：专业人员总是为以后进出留下后门，以备不时之需。

按照商业间谍的常规做法，他们把一些也许以后要用的东西放进了后口袋，然后把包含授权名单的文件复制到了软盘上，他们谁都不知道这是否有用，但是“我们已经在这儿了，不如……”，事后常常证明了这样做的好处。

第二天，其中一人打电话到存储公司，使用他们添加到授权名单上的名字和相应的密码通过了验证，然后请求提取詹金斯与派屈律师事务所上个月所有的磁带，并说将会有信使服务来拿包裹。大概下午三点，安德雷森拿到了那些磁带，他的人把所有的数据复制到了他们自己的电脑系统上，准备在空闲时间进行搜索。让安德雷森感到高兴的是，律师事务所和其它大多数商业公司一样，并没有加密他们的备份数据。

磁带在第二天就送回了存储公司，没有引起任何人的注意。

米特尼克语录

有价值的信息无论在哪儿都必须受到保护（不管是哪种形式）。一家公司的客户名单，不管是存储箱里印刷文档还是办公室的电子文档，具有同样的价值。社会工程师总是喜欢轻松地绕

开安全措施，选择最薄弱的环节作为攻击目标。窃取一家公司的异地备份储存设备被发现或被抓住的风险很低，每一家公司在存储任何有价值、敏感或者关键的数据之前，都应当将其加密以保护数据的机密性。

过程分析

因为松懈的物理安全，坏人们轻易地打开了存储公司的锁，获得了计算机的访问权限，然后修改了包含存储室授权名单的数据库，用名单上伪造的名字获得了他们需要的计算机备份磁带，而不是闯入这家公司的存储室。因为大多数的商业公司没有加密备份数据，他们得到的是可用的信息。

一家没有采取合理的安全措施的服务公司让攻击者轻易地获得了他们的客户信息资源，这只是其中的一个例子。

新的商业伙伴

社会工程师比起骗子来有一个巨大的优势，那就是距离。骗子骗你的时候你肯定在场，你可以对他有一个直观的描述，如果你发现得早，甚至还可以打电话叫警察。

社会工程师通常会像躲避瘟疫一样躲避风险，但是有时候必须要冒一定的风险，为了潜在的回报，这样做是值得的。

杰西卡的故事

杰西卡安多弗（Jessica Andover）对自己在快车数控公司的工作非常满意，当然了，一切才刚刚开始，他们付的钱不多，但是这里的人都很友好，并且她很兴奋地了解到她的员工认股权能够让她变得有钱，也许不会像公司创始人那样成为百万富翁，但是对她而言，这已经足够了。

八月的星期二上午，瑞克戴高特（Rick Daggot）一走进大厅就收到了一个灿烂的微笑，昂贵的衣服（阿玛尼）和重金表（劳力士），完美的发型，他的男子气概和自信在杰西卡的高中时代足够让所有的女生为之疯狂。

“你好，”他说：“我是瑞克戴高特，我找拉里。”

杰西卡淡淡地微笑，“拉里？”她说，“拉里这个星期休假。”“我和他约在一点，我刚从路易斯维尔飞过来。”瑞克说，然后他拿出他的掌上电脑，把它打开来给她看。

她看了一下然后轻轻地摇了摇头。“20号，”她说，“是下个星期。”他把掌上电脑收回来仔细看了看，“喔，不！”他惊叹道，“真不敢相信我犯了这么愚蠢的错误。”

“我帮你订回程机票吧，好吗？”她很同情瑞克。

在她打电话的时候，瑞克说他和拉里准备建立战略营销同

盟，瑞克的公司为生产装配线制造的产品可以和他们的新产品C2Alpha完美的结合起来。瑞克的产品与C2Alpha的合作将为两家公司打开重要的工业市场。

当杰西卡预定好下午晚些时候的航班时，瑞克说，“好吧，至少我可以和史蒂夫谈谈，如果他在的话。”但是史蒂夫，这家公司的副总裁和共同创办人，通常都不在办公室。

瑞克很友好地和杰西卡开了几个玩笑，然后暗示在下午回去之前他还有很多时间，他可以和一些关键人物一起吃午餐，接着他补充道，“当然，也包括你——如果没有其他人邀请你共进午餐的话。”

瑞克很友好地和杰西卡开了几个玩笑，然后提出他可以和一些关键人物一起吃午餐，在下午回去之前他还有很多时间。“当然，也包括你——如果没有其他人邀请你共进午餐的话。”他补充道。

杰西卡明白了这句话的意思，面色有些红晕，她问，“你想要哪些人来？”他再一次打开了他的掌上电脑，然后列举了一些人的名字——研发部（R&D）的两个工程师，新来的营销员，还有负责项目经费的财务人员。瑞克建议她告诉他们他和这家公司之间的关系，并且他想向他们介绍自己。他说出了这一区最好的餐厅的名字，那是杰西卡一直想去的地方，他说他已经订好了12:30的桌子，上午晚些时候他会打电话来确认事情都已经安排好了。

当他们聚集在餐厅的时候——他们四个加上杰西卡，他们的桌子还没准备好，所以他们在吧台旁边坐了下来，瑞克很清楚地表示饮料和午餐都算他的。瑞克很有风度也很合群，是那种刚见面就让人觉得很舒服的人，你甚至会觉得已经认识他很多年了。他似乎总是知道应该说什么好，在冷场的时候总是能进行生动的评论或者谈论一些有趣的东西，让人觉得有他在真好。

他共享了一些他自己公司的产品资料，足以让他们对合作方案展开想像。他举出了几个已经成为他的公司客户的财富500强公司，然后所有人都开始想像他们的产品一经推出就大受欢迎的样子。

然后瑞克走向了其中一个工程师布莱恩。当其他人各自聊着天的时候，瑞克私下里和布莱恩进行了交流，布莱恩向他的描述了C2Alpha的特色和一些其它竞争者没有的功能，他发现了几个布莱恩非常喜欢并认为“非常棒”但没有得到公司重视的功能。

瑞克一个一个地走过去和他们聊天，那个营销员为自己有机会谈论首次展出日期和销售计划而感到高兴，而精于计算的瑞克则从口袋里拿出了一个信封，详细地写下了生产成本、价格底线、预期盈利和每一个供应商（按名称排列）的销售价格。

当他们的桌子准备好的时候，瑞克和每一个人都交换了看法

并赢得了大家的尊敬。在午餐的最后，他们依次和瑞克握手并向他表示感谢，而瑞克则和他们交换了各自的名片，顺便和布莱恩（那个工程师）提起他想在拉里回来的时候和他进行深入的讨论。

第二天布莱恩就接到了瑞克的电话，他说他刚和拉里通完话。“我星期一会来和他讨论一些具体的问题，”瑞克说，“他想让我为你们的产品提速，他要你把最新的设计与规格Email给他，他会从中挑选要转交给我的部分。”

布莱恩说没问题，瑞克继续说道，“拉里想告诉你他的常用邮箱出了问题，无法接收Email，为此他在宾馆的商务中心申请了一个Yahoo邮箱帐号，他说你可以把文件发送到larryrobotics@yahoo.com。”

星期一上午，当拉里轻松地走进办公室的时候，杰西卡正在滔滔不绝地说着瑞克，“他人真好，请了好多人一起吃午餐，连我都去了。”拉里一脸的茫然，“瑞克？那该死的瑞克是谁？”

“你在说什么啊？他是你的商业伙伴啊。”“什么！！！？？？”

“所有人对他印象都很深，他问了一些很好的问题。”“我不认识什么瑞克……”

“你怎么了？你在开玩笑吗？拉里——你是在忽悠我，对吧？”

“让所有的主管到会议室来，马上，不管他们在做什么，还有每一个去吃了那餐饭的人，包括你。”

他们忧郁地坐在桌子四周，几乎没有人说话。拉里走进会议室，说，“我不认识这个叫瑞克的人，也没有什么新的商业伙伴，这件事我是最后一个知道的，我认为这很明显了，如果这是我们中的某个人开的玩笑，我希望他现在大声地说出来。”

鸦雀无声，会议室陷入了沉寂。

最终，布莱恩说话了，“为什么我发产品规格和源代码的email给你的时候你不说呢？”

“什么email？”

布莱恩呆住了，“噢，该死的！”

克利夫，另一个工程师，插话说，“他给了我们所有人名片，我们只要打电话给他看看到底是怎么回事。”

布莱恩拿出他的掌上电脑，调出一条记录，并把它递给桌子对面的拉里。当拉里拨电话的时候，他们还抱着一线希望，所有人都出神地看着拉里。片刻之后，他按下了免提键，所有人都听到了电话里的忙音。在超过20分钟的时间尝试拨打这个号码几次之后，拉里只好打给接线员请求紧急中断。

几分钟后，接线员的声音出现在了电话里，她用质问的口气

说，“先生，你从哪儿得到的这个号码？”拉里告诉她是从一个他很想联系上的人的名片上，接线员说，“我很抱歉，这是电话公司的测试号码，永远都是忙音。”

拉里开始列举瑞克得到的信息，情况不容乐观。

两个便衣警察来做了笔录，在听了这个故事之后，他们指出这没有违反任何州法，他们帮不上忙。他们建议拉里联系FBI，因为他们有权制止任何涉及州际贸易的犯罪行为。当瑞克戴高特伪造身份让工程师寄出测试结果时，他可能违反了一项联邦法律，但是要等到瑞克和FBI谈话的时候才知道

三个月后，当拉里吃完早餐在厨房读早报的时候，他的咖啡差一点洒了出来，自从他第一次听到关于瑞克的事以后就一直在担心，而现在，他最坏的恶梦变成了现实。商业版的头条上白纸黑字写着：一家他从未听说过的公司发布了一个新产品，似乎很像是他的公司已经开发了两年的C2Alpha。

通过骗局，这些人在市场上打败了他，他的梦想破灭了。投资研发的百万美元浪费了，他还找不到任何证据证明是他们干的。

山米桑福德的故事

足够聪明，找一份高薪工作不是问题，但是不够安分，宁愿靠行骗谋生，山米桑福德（Sammy Sanford）一直做得非常好，直到他遇见了一个因饮酒问题而被迫提前退休的特工，这个人已经找到了用政府要求他熟练的技能赚钱的方法，他一直在寻找能用的人，然后他发现了山米，在他们第一次见面的时候。山米觉得这很简单，回报也很高，就把他的重心从诈骗转移到了盗窃公司机密上。

大部分人不知道我在做什么。通过电话或者互联网和人们聊天，任何时候都不会有人看见你，但是任何一个优秀的骗子，都能够用传统的、面对面的方式撒下弥天大谎，并让你相信它（现在还有很多这样的人，超乎你的想像）。我认识的一个检察官认为这是犯罪，但我觉得这是一种天分。

但是你不能盲目前进，首先你必须制定计划。在街头行骗中，你可以用友好的对话试探目标，然后措辞小心地提出建议，如果得到了正面的回应，嘿！——你就抓住了一只鸽子。

公司任务和我们的大型骗局差不多，你得要一步一步来，找出他们的“按钮”，了解他们想要什么、需要什么，制定攻击计划，耐心地做你的功课，了解你将要扮演的角色，背好台词，在你做好准备之前不要走进那张门。

我花了三个星期调查目标，然后与客户商讨了两天怎样介

绍“我的”公司和怎样解释两家公司的商业合作联盟。

接下来的事情很顺利，我打电话到那家公司说我是风险投资公司的，我们要安排一次会议，我想在下个月找出一个所有股东都用空的时间，有没有我应该避开的、拉里的不在的时间段？然后她说，自从他们创办了这家公司以来，两年里他几乎没有休息过，但是这一次他的妻子把他拽了出来，他会在八月的第一个星期度过一个高尔夫假期。

离现在还有两个星期，我可以等。

在此期间一家业内杂志给了我该企业的公关公司名称，我说我很喜欢他们为数控公司提供的服务，我想让同一个人负责我的公司，结果我见到了一位精力充沛的年轻女士，她大概认为她会得到一个新的客户。在一顿昂贵的午餐（她实际上并不想要这么多酒，但是我想喝）上，她尽全力让我相信他们非常擅于理解客户的问题并找出正确的公关解决方案。我假装不是很相信，想得到一些详细的资料。在我的提醒下，她把新产品的很多情况和这家公司的一些问题全都告诉了我，超出了我的预期目标。

事情发展得很顺利，因为我的“失误”，到了那里才发现会议在下个星期，但是我想在这段时间里和公司的团队见一下面，接待员轻易地相信了我，她甚至同情起了我。午餐花了我足足150美元，包括小费，但是我得到了我想要的东西，电话号码、工作头衔和一个关键人物的信任。

布莱恩被我给骗了，我承认。他看上去就像是那种会把所有我请求的资料发给我的人，但是当我说出项目名称时，听上去他还是犹豫了一会儿，这在意料之中。那个email账户用的是拉里的名字，为了以防万一，我把它放在了后口袋里。Yahoo的安全人员也许还期待着有人再次登录那个账户好让他们追踪他，他们可有得等了。胖妞开始唱歌了，我又有新的任务了。

过程分析

任何街头骗子都能够很好地伪装自己，他会让自己在赛马场是一个样子，在当地的酒吧是一个样子，在梦幻旅馆的高消费吧台又是另一个样子。

这对商业间谍而言是一样的。如果要伪装成一家公司的主管、顾问或者销售代表，一套合适的衣服和领带是少不了的，当然，还要有一个昂贵的公文包。在不同的任务中，扮演软件工程师、技术人员或者邮件收发员所穿的衣服（或制服）都各不相同。

为了渗透进这家公司，这个自称是瑞克戴高特的人知道他必须表现出足够的自信和能力，之前他就已经对这家公司的产品和整个行业做了充分的调查。

要得到他需要的信息并不很难。他发现了一个简单的方法可以找出这家公司的CEO外出的时间。要找到足够的工程资料是个小小的挑战，但不是很难，这让他可以了解他们在做什么的“内部消息”。这些信息通常可以从很多地方获得，比如各种各样的服务公司、投资者、风险投资商、他们的银行家和他们的律师事务所。尽管如此，攻击者还是很小心：如果找对了人还好，要是两三次遇到不配合的人，就会有被发觉的危险。这条路充满了危险，所有的瑞克戴高特都需要谨慎地选择并遵守每条路只走一次的法则。

午餐是另一件难事。首先他要安排一段时间和每个人单独相处，在别人听不到的地方。他告诉杰西卡的时间是12:30，但是却在一家高消费的餐厅订了下午1点的桌子。按照他的计划，他们不得不在吧台上喝东西，这样一来，他就可以到处走动和每个人单独聊天了。

尽管如此，瑞克还是有被发现的危险——只要一句错误的回答或者粗心的评论就够了。只有无比自信和狡猾的商业间谍才敢冒这样的险，但是多年街头行骗的经验让瑞克充满了自信，即使出现失误，他也可以很好的掩饰并消除任何怀疑。这是整个行动中最有挑战性，也是最危险的一部分，完成像这样的骗局让他清楚地认识到，为什么他没有飚车、跳伞或者婚外恋——因为这份工作让他充满了激情。有多少人能像他一样？他想知道。

米特尼克语录

虽然大部分的社会工程学攻击都出现在电话或email上，但是不要认为不会有胆大的攻击者出现在你的公司。在大多数情况下，行骗者能够用普通的常用软件，比如Photoshop，伪造一张员工证件进入大楼。

写有电话公司测试专线的名片是怎么来的？在《罗克福德档案》（关于一个聪明、幽默的私家侦探的故事）中，罗克福德（由James Garner扮演）的车上有一部便携式名片印刷机，他可以在不同的地方打印不同的名片。现在，社会工程师可以到复印店打印名片，或者用激光打印机打印。

注释

《冷战谍魂》、《完美间谍》等优秀小说的作者约翰勒卡雷（John Le Carre）讲述了许多完美、动人的故事。勒卡雷在很小的时候就认识到，被他父亲骗了的人，通常很容易受骗，并且会被骗很多次。这正说明每个人都有可能被社会工程师利用。

是什么让一群聪明人接受了一个骗子？综合起来，是因为骗

子塑造了一个可信的形象，而我们通常会因此放松警惕。一个成功的骗子（或社会工程师）与失败者的差距就这里。

问问你自己有多大的把握不会被瑞克的故事吸引？如果你确定你不会，那就问有没有人曾经成功地欺骗过你，如果第二个问题的回答是有，或许第一个问题的正确答案也一样。

跳背游戏

下面的故事并不涉及商业间谍活动，在你阅读的时候，试着去理解为什么我要把它放在这一章！

哈里塔迪（Harry Tardy）被送回家了，他心情很不好。海军陆战队似乎早就准备好了要刷下一大批人，在他被踢出新兵营之前。现在他回到了他痛恨的家乡，在当地的社区大学进修计算机课程，并寻找着向这个世界发泄的机会。最终他想出了一个计划。在和一个同班同学喝了几杯啤酒之后，他开始抱怨他们的导师，一个自认为无所不知的人，然后他们一起制定了一个缺德的计划来戏弄他：他们要弄到一款掌上电脑（PDA）的源代码并把它放进他们导师的电脑里，然后留下线索让PDA公司的人找到“做坏事”的人。

这位新朋友，卡尔亚历山大（Karl Alexander），说他“知道一些骗局”，并告诉了哈里具体的实现方法。乏味的是，他们又成功了。

完成他们的家庭作业

经过前期调查之后，哈里发现该产品主要是在PDA厂商的海外总部开发的，但是在美国也有一家研发机构。这很好，卡尔指出，这家研发公司肯定也需要访问产品的源代码。

然后哈里准备打电话到海外的研发中心，上演一场同情心大作战，“哎呀，我遇到麻烦了，拜托，拜托，帮帮我。”卡尔写了一个剧本，但是哈里似乎不能搞定这些台词，最后他和卡尔一起进行了练习，学会了他所需要的谈话语气。

最终哈里是这样说的（卡尔坐在他的旁边）：

“明尼阿波利斯研发中心，我们整个部门的服务器全都感染了蠕虫病毒，我们只好重新安装了操作系统，然后当我们从备份数据恢复的时候，我们发现没有一个是能用的。猜猜是谁对这些备份数据的完整性负责？正是我。我刚被我的上司教训了一顿，管理人员对我们失去了这些数据感到很生气。你看，我需要最近修订的完整的源代码，我希望你能够尽快地gzip（压缩）源代码并它发给我。”

这时卡尔草草地写了张纸条给他，然后哈里告诉电话另一头的人，他只是想让他把文件发送到明尼阿波利斯研发中心。这一

点非常重要：当电话里的这个人认为他只不过是把文件发到公司的另一个地方去，他的心里就会觉得很踏实——这样能出什么问题呢？

注释

GZIP：使用一个Linux　GNU工具把多个文件压缩到一个单独的文件中。

他答应了。在卡尔的帮助下，哈里一步步地指引电话里的人把庞大的源代码压缩到一个单一的、紧凑的文件中去，他还给了他一个文件名，“newdata”，并解释说这样可以避免与他们被破坏的旧数据混淆。

卡尔把下一个步骤解释了两遍哈里才明白过来，这是卡尔精心设计的跳背小游戏中十分关键的一部分，哈里打电话到明尼阿波利斯研发部，对某个人说“我想发一个文件给你，请你帮忙转发到另一个地方”——一个合理的借口当然是少不了的。令哈里感到困惑的是：他需要说“我会发送一个文件给你”，但是他根本就没有发送。当研发中心真的收到从欧洲发来的产品源代码时，他必须让电话里的人认为那个文件是他发来的。“为什么我要告诉他那个文件是我发的？不是从国外发来的吗？”哈里想知道。

“关键是研发中心的那个人，”卡尔解释说，“他会认为他只是在帮一个美国同事的忙，从你那里收到文件并帮你转发出去。”

哈里最终明白了。他打电话到研发公司让接线员帮他转接到电脑中心，然后请求和电脑操作员谈话。一个听上去和哈里一样年轻的人拿起了电话，哈里向他表示了问候并解释说他是芝加哥制造分公司的，他要发送一个文件给他们的合作伙伴，项目才能继续下去，但是，他说，“我们的路由器出了问题，无法连接到他们的网络，我想把文件先传给你，在你收到之后，我会打电话告诉你怎样转发给我们的合作伙伴。”

到目前为止，一切都很顺利。接着，哈里询问那个年轻人电脑中心是否有匿名FTP（允许任何人上传或下载文件而无需密码）账户，得到的回答是有一个匿名FTP，然后他把内部的Internet协议（IP）地址告诉了哈里。

注释

匿名FTP：无需账户也能通过文件传输协议（FTP）访问远程计算机。虽然匿名FTP可以在没有密码的情况下访问，但是用户的访问权限通常会限制在几个指定的文件夹内。

得到这一信息之后，哈里又打电话到了海外的研发中心，这

时压缩文件已经准备好了，于是哈里指引电话里的人把文件上传到那个匿名的FTP站点，不到五分钟，研发中心的年轻人就收到了被压缩的源代码文件。

设定受害人

计划已经完成了一半，现在哈里和卡尔需要等待并确认文件已经到达，利用这段时间，他们穿过房间走到导师的办公桌旁，开始实施另外两个必要的步骤。首先他们在他的机器上设置了一个匿名FTP服务器作为计划中的文件传输终点站。

而第二步则解决了另一个难题。显然他们不能告诉研发中心的人把文件发送到一个像这样的地址，warren@rms.ca.edu，“edu”域名将成为死穴，即使是半清醒的电脑人员也会认出这是学校的地址，整个行动都将暴露无遗。为了避免出现这种情况，他们进入了导师的Windows系统，查看了他的IP地址，他们会用它来发送文件。

现在是时候回电给研发中心的电脑操作员了，哈里在电话里对他说，“我刚刚上传了我跟你说的那个文件，你看一下有没有？”

有，收到了。于是哈里要他转发文件，并说出了IP地址。当这个年轻人开始连接并传送文件的时候，哈里一直拿着电话，然后他们开心地看见穿过房间导师的电脑硬盘指示灯不停地闪啊闪——忙着接收文件。

哈里和那个人交换了一些看法，关于电脑和外围设备怎样才能更加可靠，然后向他表示了谢意并说，再见。

两人把导师机器里的文件复制了一份到两张Zip磁盘上，每人一张，这样以后他们就可以拿出来看看，就像是从博物馆偷来的一副油画，你可以自己欣赏，却不能把它给你的朋友们看。除此之外，在这种情况下，他们更像是偷了一副油画的复制品，而原画仍在博物馆那里。

然后卡尔让哈里移除导师机器上的FTP服务器并抹去日志文件，这样就没有任何证据证明是他们做的——只剩下放在显著位置上的源代码文件。

作为最后一步，他们直接在导师的电脑上把部分源代码提交到了Usenet，只有一部分，不会对那家公司造成任何重大损失，但是能留下足够清晰的痕迹，他们的导师恐怕要解释一些难以解释的事情了。

过程分析

虽然实施这种恶作剧需要很多方面的知识，但绝对少不了赢得同情和帮助的精彩表演：我被我的上司教训了一顿，管理人员

很生气，等等，再加上对电话另一头的人说，你可以怎样怎样帮助我解决这个问题，这是一种十分有说服力的骗局，在这里有效，并且在其它许多地方也有效。

第二个关键要素是：这个人知道这些文件的价值并把它发送到了一个公司内部的地址。

第三个值得思考的问题是：电脑操作员可以看到这个文件是从公司内部发来的，这就意味着——或者看上去如此——这个把文件发给他的人，其实可以自己把文件发送到最终目的地去，只要他的外部网络连接还能用的话。帮他发送一个文件能出什么问题呢？

为什么要更改压缩后的文件名呢？这似乎只是个小步骤，但事实上非常重要，攻击者不能让写有"源代码"字样（或者涉及到产品的名字）的文件直接发送出去，请求发送这样的文件可能会引发警报，选择用一个无关紧要的名字对文件重命名非常重要。就像攻击者设计的那样，第二个年轻人毫不犹豫地把文件发送到了公司外部：一个new　data文件，没有任何可以查看的真实文件信息，很难让人产生怀疑。

米特尼克语录

每一个员工都应该牢牢地记住下面这条规定：除非得到管理人员同意，不要把文件发送给任何你不认识的人，即使目的地似乎是你们公司的内部网络。

最终，你找出上面这个故事与商业间谍活动的联系了吗？如果没有，请看答案：这两个学生的恶作剧行为专业的商业间谍可以轻易地完成，或者受雇于竞争对手，或者受雇于国外政府，无论是哪种方式，都能对公司造成巨大的损失，如果市场上提前出现同类产品，将严重损害他们新产品的销售。

对你的公司实施同种类型的攻击有多么容易？

防范措施

长久以来一直困扰着企业的商业间谍活动，现在已经成为了传统间谍的谋生手段。冷战已经结束了，外国政府和企业现在正利用独立的商业间谍窃取信息。国内的公司同样也雇用违法的信息猎手获取竞争对手的情报。在很多种情况下，曾经的军事间谍成为了商业信息猎手，他们有足够的知识与经验，可以轻易地渗透企业，特别是那些没有训练员工并且未能配置安全措施保护他们的信息的企业。

远距离安全

有什么可以帮助遇到异地存储设施问题的公司？这种威胁本来是可以消除的，如果这家公司加密了他们的数据的话。没错，加密需要额外的时间和费用，但这样做非常值得。已加密文件需要定期抽查以确认文件能够正常加密/解密。

总是有密钥丢失的危险，或者惟一一个知道密钥的人出了车祸，但是危险等级被最小化了。把敏感文件放在存储公司又不将其加密的人，恕我直言，是个白痴。这就像是走在治安不好的街道上，把口袋里的20美元露出来，摆明了要让别人抢。

在不安全的地方留下备份媒体可以说是安全通病了。几年以前，我在一家本来可以更好地保护他们的客户资料的公司工作。业务人员每天都会把备份磁盘放在锁住了的机房外边给信使取，任何人都能够顺手牵羊带走这张备份磁盘，里面有这家公司所有的文字处理文档，并且没有加密。如果备份数据被加密了，丢失磁盘只是件麻烦的事情，如果没有被加密——你应该比我更清楚这将对公司造成什么样的影响。

大一点的公司对可靠的异地存储的需要几乎是毋庸置疑的，但是你的公司的安全程序需要包含一项对合作的存储公司的调查，看他们的安全策略和做法是否到位，如果他们没有关注这些，你在安全方面的所有努力可能都白费了。

小一点的公司则有更好的备份选择：每天晚上把新文件和更改过的文件发送到一个提供在线存储的公司去。重复一次，必须要对数据进行加密。另外，并不是只有存储公司的员工可以接触到这些文件，每一个成功入侵这家在线存储公司的计算机系统或网络的入侵者都可以。

当然，当你设置了加密系统保护你的备份文件安全时，你还必须设置一个高度安全的程序存储解开它们的加密密匙或者密码短语，常用于加密数据密匙应当存储在一个安全或者密封的地方。标准的公司程序需要应对一些可能性，比如处理这些数据的员工突然离职、去世或者跳槽，必须要有至少两个人知道这个存储地点和加密/解密程序，以及规定什么时候和怎样更改密码，曾经管理加密密匙的员工离职之后必须马上更改密码。

那是谁？

在这一章中的举例中，聪明的行骗艺术家利用个人魅力获取员工的信任，因此身份验证变得更加重要。能否响应将源代码发送到一个FTP站点的请求，关键是你是否了解请求者。

在第十六章中，你将看到详细的身份验证策略，以应对请求信息或者执行某项操作的陌生人，我们已经在这本书里讨论过很多次身份验证的必要性了：在第十六章你将了解应该如何去做。

第四部分加强防范

第十五章 信息安全知识与培训

一个社会工程师已经关注你的新产品发布计划两个月了。

有什么能阻止他？

你的防火墙？不行。

强悍的验证设备？不行。入侵检测系统？不行。加密？不行。

限制调制解调器的访问？不行。

编码服务器名称，使入侵者无法确定产品计划所在的服务器？不行。

事实上，没有任何技术能防范社会工程学攻击。

安全技术、培训和程序

许多公司在他们的安全渗透测试报告中说，他们对客户公司计算机系统实施的社会工程学攻击几乎可以百分之百成功。使用安全技术的确可以让这些攻击更难实施，但唯一真正有效的办法是，将安全技术和安全策略结合起来，规范员工行为并适当地进行培训。

只有一种方法能让你的产品计划安全，那就是接受过安全培训的负责任的员工。这不仅涉及到安全策略和安全程序的培训，还包括了安全知识的培训。一些权威人士建议把公司40%的安全预算用在安全知识的培训上。

第一步是让企业的每一个人都认识到那些能操纵他们心理的人的存在，员工们必须了解信息需要哪些保护与如何保护。当人们了解了操纵的细节时，他们便能在攻击初期更好地处理。

安全培训也意味着让企业的所有员工了解公司的安全策略与程序，就像在第17章所讨论的那样，策略是指导员工行为保护企业信息系统与敏感信息所必须的规则。

本章和下一章提供了一张把你从可怕的攻击中解救出来的安全蓝图。如果你没有培训并警告员工遵循谨慎考虑过的程序，这也许没什么大不了的，在你被社会工程师窃取贵重信息之前。不要等到攻击发生才制定这些策略：这对你的事业和你的员工福利将是毁灭性的。

了解攻击者是怎样利用人的天性的

为了制定一套成功的培训程序，首先你必须了解为什么人们容易遭受攻击，在你的培训中识别这些倾向--比如，通过角色扮演讨论引起他们的注意--你能帮助你的员工了解为什么我们都能被社会工程师轻易地操纵。

社会科学家对心理操纵的研究至少已经有50年了，罗伯特B

西奥迪尼（Robert B Cialdini）在科学美国人（2001年2月）杂志中总结了这些研究，介绍了6种"人类天性基本倾向"。

这6种倾向正是社会工程师在他们的攻击尝试中所依赖的（有意识的或者无意识的）。

权威

当请求来自权威人士时，人们有一种顺从的倾向。就像本书其它地方所讨论的那样，如果人们相信请求者是权威人士或有权进行这样的请求的人，他（或她）便会毫不怀疑地执行请求。

在西奥迪尼博士写的一篇论文中，一个声称是医院医师的人打电话给三家中西部医院的22个独立护士站要求她们为病房的一个病人送去处方药，收到这些命令的护士们根本不认识呼叫者，她们甚至不知道他是否真的是医师（他不是），她们是从电话里收到处方药的命令的，这显然违背了医院的策略。她们被要求送给病人的药物是未授权，并且剂量是每日最大剂量的两倍，这足够危及病人的生命了。然而在95%的案例中，西奥迪尼写道，"护士从病房医药箱中取出了足够的剂量并把它给了病人。"之后观察者阻止了护士并解释这是一次实验。

攻击举例：一个社会工程师试图伪装成IT部门的权威人士，声称他是公司的主管（或者为主管工作的人）。

爱好

当作出请求的人很可爱或者与被请求者有相同的爱好、信仰和意见是，人们总是倾向于顺从。

攻击举例：通过交谈，攻击者设法了解了目标的兴趣或爱好，并声称他也有相同的兴趣或爱好，或者来自于同一个州或学校，或者有相似的目标。社会工程师还会尝试模仿目标的行为创造相似性。

报答

当我们被给予（或者许诺）了一些有价值的东西时，我们可能会自动地同意请求。礼物可以是资料、建议、或帮助，当有人为你做了一些事情时，你会倾向于报答他。这种强烈的报答倾向甚至在你收到了并不需要的礼物时依然存在。让人们"帮忙"（同意请求）的最有效的方法之一就是给予一些礼物形成潜在的债务。

哈瑞奎师那教徒善于此道，他们会送书籍或者鲜花作为礼物，然后等待回报。如果收到礼物的人想要归还礼物，给予者便会拒绝并说明，"这是我们给你的礼物。"这一回报行为法则被奎师那教徒们用在了增加捐款上。

攻击举例：一个员工接到了自称是IT部门的人的电话，呼叫者解释说公司的一些电脑感染了还没有被杀毒软件识别的破坏电脑文件的新病毒，并建议他进行一些步骤来防御病毒。在这之后，呼叫者让他测试了一个允许用户更改密码的加强版软件程序，这名员工很难拒绝，因为呼叫者是在帮助他防御病毒，他的回报就是响应呼叫者的请求。

守信

当人们公开承诺了或者认可了一些事情时，会倾向于顺从。一旦我们承诺了一些事情，为了避免自己成为不可信赖或者不受欢迎的人，我们会倾向于坚持我们的立场或承诺。

攻击举例：攻击者联系上了一个新员工并提醒她遵守某些安全策略与程序，比如允许使用公司信息系统的情况。在讨论了一些安全规定之后，呼叫者向用户请求她的密码进行"灵活度检查"以选择高强度的密码。一旦用户说出了她的密码，呼叫者便会提出一些创建密码的建议使攻击者无法猜测密码。受害人顺从了，因为她之前已经答应遵守公司的策略，并且她认为呼叫者只不过是在帮她检查密码是否合适。

社会认可

当要做的事情看上去和别人所做的事情一样的时候，人们会倾向于顺应请求。当其他人也这样做时，人们就会认为这些（值得怀疑的）行为是正确的。

攻击举例：呼叫者说他正在进行一次调查并说出了部门中的其他人的名字，他声称这些人已经和他合作过了。受害人相信其他人已经确认了这一请求的合法性，于是呼叫者问了一系列的问题，其中一项引导受害人说出他的计算机用户名和密码。

短缺

当人们相信物品供应不足并且有其他竞争者（或者只在短时间内有效）时，便会倾向于顺应请求。

攻击举例：攻击者发送了一封email声称在公司的新网站上注册的前500个人将赢得一部热门电影的电影票。当一名毫不怀疑的员工在该网站上注册时，他会要求提供他的公司email地址并选择一个密码。有很多人为了方便，总是倾向于在他们使用的每一个计算机系统上使用相同或相似的密码，利用这一点，攻击者便能使用此用户名和密码（在网站注册过程中填写的）攻击目标的工作或家庭计算机系统。

创建培训程序

发行一本安全策略手册或者让员工关注企业内网上的安全策略资料，这些都不会单独减少你面对的威胁。每一家商业公司都必须写下这些策略详细地制定规则，而且必须对涉及企业信息或计算机系统的每一个人进行额外的引导，让他们学习并遵循这些规则。此外，你还必须确保他们理解了每一条策略的制定原因，这样他们才不会为了方便而绕过这些规则。另外，员工的借口永远都是"不了解"，而这正是社会工程师所利用的弱点。

任何安全识别程序的首要目标都是影响人们改变他们的行为和态度，鼓励员工参与到企业信息资产的保护中来。在这种情况下的一种很好的激励方式是向员工解释他们的行为不仅能让公司受益，对他们个人也很有好处。如果公司对每一位员工都保留了一些隐私信息，那么当员工们尽职保护信息或信息系统时，他们事实上也保护了他们自己的信息。

安全培训程序需要覆盖允许访问敏感信息或企业计算机系统的每一个人，必须正在实施，还必须不断地修订与更新以应对新的威胁和攻击，员工们必须看到高级管理人员完全遵守了程序规定，承诺必须是真实的，而不是橡皮盖章的"我们承诺"备忘录，并且程序还必须有足够的资源支持其发展、通信与测试。

目标

发展信息安全知识与培训程序的基本原则是让所有员工意识到他们的公司在任何时候都有可能遭受攻击。他们必须认识到每一个员工都扮演着保护计算机系统或敏感数据的重要角色。

因为信息安全在很多方面都涉及到了技术，所以员工会轻易地认为问题已经被防火墙或其它安全工具处理了。培训的一个主要目标就是让每一个员工认识到他们处在保护企业整体安全的最前沿。

安全培训必须要有一个深入的、较大的目标，而不是简单地制定规则。培训程序设计者必须认识员工所面对的巨大的诱惑，为了完成工作而忽略他们的安全职责。了解社会工程学策略和怎样防范攻击非常重要，但这只在培训程序激发了员工使用这些知识的情况下才有效。

公司可以用一个类似于会议基本目标的概念来判断培训程序是否有效：在结束培训之后，他（或她）是否认为信息安全是他（或她）的工作之一。

员工们必须认识到来自社会工程学的威胁是真实的，敏感企业信息的损失会危及到公司和他们自己的个人信息。在某种意义上说，忽视信息安全相当于泄漏某人的自动取款机PIN码或者信用卡号，类似的比喻可以增加员工培养安全习惯的积极性。

## 建立知识与培训程序

负责设计信息安全程序的人必须认识到这不是一个一刀切的项目，培训程序需要适应企业内不同组的特殊需要。在16章描述的许多安全策略都是全体适用的，而很多其它的策略是针对指定员工组的。大部分公司的培训程序都需要适应以下这些组：管理人员、IT职员、计算机用户、非技术人员、行政助理、接待员和安全警卫。（请看第16章，根据工作分配分解策略）

因为公司的商业安全警卫通常并不精通电脑，并且，他们接触公司电脑的几率很小，所以在设计培训程序时通常不会考虑他们。但是，社会工程师可以欺骗安全警卫或其他人放他们进大楼或办公室，或者让他们协助实施计算机入侵。警卫当然不需要像操作电脑的人那样参加全部的培训，但是他们必须了解安全知识程序。

在企业内部或许会有哪些是所有员工都需要培训的重要、固有的安全缺陷，设计优秀的信息安全培训程序必须获知并捕捉学习者的积极性和注意力。

信息安全知识与培训的目标应当包括一次迷人的交互式体验，可以通过角色扮演演示社会工程学攻击，评价最近媒体对那些不幸的公司的攻击报导，讨论这些公司怎样才能避免损失，或者播放既生动又有教育性的安全视频，有几家安全公司销售这些视频和相关的资料。

注释

对于那些没有资源开发内部程序的公司，有几家培训公司提供安全知识培训服务，可以在Secure World Expo (www.secureworldexpo.com)上找到这些公司的信息。

本书中的故事提供了许多材料说明社会工程学方法和策略来加强威胁意识，展示人类行为的弱点，可以考虑使用他们的方案进行角色扮演活动，这些故事同时也提供了有趣的讨论机会，比如受害者可以怎样回应来抵御攻击。

熟练的课程设计者和熟练的讲师会发现很多挑战，但也有很多机会让课堂活跃起来，还可以在此过程中促使人们成为解决方案的一部分。

## 培训结构

所有员工都必须参加基本的安全知识培训程序，新员工必须参加培训作为他们的初始教育，我建议规定新员工不能接触公司的计算机系统，直到他们完成了基础安全知识课程。

对于初始的安全知识培训，我建议简短一些，但能引起足够的注意力，让员工们记住重要的讯息。当因资料过多而需要长时间培训时，必须提供合理的基本讯息数量，我认为超过半天或全天的培训会让人们因信息过多而变得麻木。

这些课程的重点应当是让员工认识到自己和公司都有可能遭受攻击，除非所有员工都有很好的安全习惯。比学习指定的安全策略更重要的是激发员工对公司安全的责任心。

在员工不愿意参加教室课程的情况下，公司应当考虑进行其它形式的教学，比如录像、基于计算机的培训、在线课程或者编写材料。

在短期的初始培训课程之后，还应当设计长期课程让不同职位的员工了解特殊的漏洞与攻击技术，第二次培训至少要持续一年以上。威胁的种类与攻击的方法都在不停地变换，所以课程的内容应当不断更新，此外，人们的知识和戒心会随着时间的推移而减少，所以培训必须每隔一段时间重复一次，才能不断地加强员工的安全意识。再重申一次，培训不仅要曝光安全威胁和社会工程学策略，还要让员工了解到安全策略的重要性并使他们拥护这些策略。

管理人员必须给他们的下属一段合理的时间熟悉安全策略和程序并参加安全知识培训。员工们不应当指望在非工作时间学习安全策略或参加安全培训，新员工应当有足够的时间熟悉安全策略，在开始他们的工作之前养成良好的安全习惯。

在企业内部更换了工作岗位，涉及到访问敏感信息或计算机系统的员工同样需要完成他们新工作的安全培训程序。比如，当一个电脑操作员成了系统管理员（或者一个接待员成了行政助理）时，就需要新的培训。

培训课程内容

在归纳基本原理的时候，所有的社会工程学攻击都有一个共同元素：欺骗。受害者相信攻击者是同一家公司的员工或者有权访问敏感信息的其他人，或者有权指挥受害者操作一台计算机或计算机相关的设备。只要员工简单地进行以下两个步骤，就可以防范几乎所有的这些攻击：

核实请求者的身份：进行请求的这个人是他所声称的那个人吗？

核实请求者是否已授权：这个人需要知道这些吗？他有没有被授权进行这种请求？

注释：

因为安全知识与培训是不完美的，所以最好在创建防御体系时深入地使用安全技术。技术性的安全措施要比针对员工个体的安全措施有效，比如，可以通过配置操作系统禁止员工从互联网上下载软件或使用简短的弱口令。

如果知识培训课程改变了员工的行为，那么可以用这些标准对员工进行测试请求，相应的社会工程学攻击威胁将大大减少。

一个实用的信息安全知识与培训程序应当包含以下内容：

描述攻击者怎样使用社会工程学技能行骗。

社会工程师实现他们目标的方法。

怎样识别可能的社会工程学攻击。

处理可疑请求的程序。

在哪里报告攻击企图或者成功的攻击。

质疑提出可疑请求的人的重要性，不管他声称自己是何职位。

在现实中，他们不应在没有严格验证的情况下完全相信别人，虽然他们更愿意在拿不准把别人往好处想。

对任何请求信息或操作的人进行身份验证与授权验证的重要性（第16章，"验证与授权程序"，描述了这些验证方式）。

保护敏感信息的程序，包括熟悉所有的数据分类系统。

公司的安全策略与程序的定位，保护信息与企业信息系统的重要性。

关键安全策略与它们的含义汇总。例如，指导每一个员工设定高强度的密码。

每一个员工遵守策略的职责与不服从的后果。

通过解说社会工程学介绍几种交互类型。攻击者为了达到他（或她）的目标，会非常频繁地使用不同的技术和通信方式，因此，一个成熟的培训程序应当包括以下内容的一部分或全部：

涉及到计算机和语音信箱密码的安全策略。

解密敏感信息或资料的程序。

Email使用策略，包括防范恶意代码攻击（病毒、蠕虫和特洛伊木马）的安全措施。

物理安全要求，比如佩戴证件。

在遇到未佩戴证件的人时，有询问质疑的责任。

良好的语音邮件安全习惯。

如何确定信息分类和适当的安全措施。

适当的处理敏感文档和过去存放过机密资料的计算机媒体。

同样，如果公司计划使用渗透测试来确定针对社会工程学攻

击的安全措施是否有效，应当警告员工注意这次练习，让员工们知道有时候他们会接到使用了攻击技术的电话或其它通讯，作为测试的一部分。测试的结果不会有任何惩罚，但是可能会需要一定范围内的额外培训。

# 第十六章 推荐的信息安全策略

由FBI主导的调查结果显示，超过90%的大企业和政府机构遭受过计算机入侵者的攻击，美联社在2002年4月对其进行了报导。有趣的是，只有大约三分之一的公司报导或公开了这些攻击，沉默意味着他们学到了很多东西，为了避免失去客户的信任，为了防止更多入侵者的出现，大部分的商业公司不会公开报导计算机安全事件。

似乎没有任何社会工程学攻击的统计，就算有，数据也很不可靠，在大部分情况下一家公司永远也不会知道社会工程师已经“偷走了”信息，因此许多攻击都没有记录。

有效的策略能针对大多数的社会工程学攻击类型进行防范，但是让我们现实——除非企业里每一个人都认识到安全的重要性并把它作为他（或她）的职责（遵守公司的安全策略），否则社会工程学攻击将永远是企业面临的严重威胁之一。

事实上，针对安全攻击的技术手段一直在进步，通过社会工程学途径获取私有的公司信息或渗透企业网络，这种攻击将越来越频繁并引起信息窃贼的关注。商业间谍通常会选择使用最简单同时也是最隐蔽的方法来达到他（或她）的目标。事实上，那些使用了最先进的安全技术保护计算机系统和网络的公司，可能会面对更多来自于使用社会工程学策略和方法的攻击。

本章介绍了防范社会工程学攻击的详细策略，这些策略除了针对基于技术漏洞的攻击，还涉及到几种引导信任的员工提供信息或执行操作的骗局，阻止攻击者访问敏感商业信息或企业计算机系统与网络。

## 什么是安全策略？

安全策略是指导员工行为、保护信息安全的明确指南，是安全体系中防范潜在威胁的重要组成部分，这些策略在察觉并防范社会工程学攻击时尤其有效。

有效的安全管理需要培训员工精心设计的策略和程序，然而，即使每一个员工都严格地遵守了安全策略，也无法保证防御所有的社会工程学攻击。相反，合理的目标总是能用可接受的标准减小威胁。

在这里介绍的这些策略包括了一些与社会工程学攻击无关的防范措施，之所以放在这里，是因为它们涉及到了一些攻击者常用的技术。例如， email附件攻击——可以安装特洛伊木马软件让攻击者控制受害者的电脑——就被定义为计算机入侵者频繁使用的方法。

制定程序的步骤

一个全面的信息安全程序通常从威胁评估开始：

需要保护哪些企业信息资产？

有哪些针对这些资产的具体威胁？

如果这些潜在的威胁成为现实会对企业造成哪些损失？

威胁评估的主要目标是对需要立即保护的信息资产按优先次序排列，而不是对安全措施进行成本效益分析。首先想一想，哪些资产需要首先保护，保护这些资产需要花多少钱。

高级管理人员的支出和对安全策略和信息安全程序的大力支持非常重要。正如其它的企业程序一样，如果一个安全程序成功了，管理层可以对其进行推广，前提是要有个人案例证明其有效性。员工们需要意识到信息安全和保护公司商业信息的重要性，每一个员工的工作都依赖于这一程序的成功。

设计信息安全策略蓝图的人需要以非技术员工也能轻松理解的通俗方式书写安全策略，并解释为什么这些是重要的，否则员工可能会认为一些策略是在浪费时间而对其忽略。策略书写者应当创建一份介绍这些策略的文档，并把它们分开来，因为这些策略可能会在执行的时候有小范围的修改。

另外，策略的书写者应当了解哪些安全技术能被用来进行信息安全培训。例如，大部分的操作系统都能用指定的规则（比如长度）限制用户密码。在一些公司，可以通过操作系统的本地或全局策略阻止用户下载程序。在允许的情况下，策略应当要求使用安全技术代替人为的判断。

必须忠告员工不遵守安全策略与程序的后果，应当制定并宣传违反策略的处罚。同样，要对表现优异或者发现并报告了安全事件的员工进行奖励。当一名员工受到奖励时，应当在公司范围内广泛地宣传，比如在公司时讯中写一篇文章。

安全培训程序的一个目标是传达安全策略的重要性和不遵守这些规则的后果。拜人性所赐，员工们有时候会忽略或绕过那些看上去不合理或者太费时间的策略。管理层有责任让员工们了解其重要性与制定这些策略的原因，而不是简单地告诉他们绕过策略是不允许的。

值得注意的是，信息安全策略不是固定不变的，就像商业需要变化一样，新的安全技术和新的安全漏洞使得策略在不断的修改或补充。应当加入常规的评估与更新程序，可以通过企业内网或公共文件夹让企业安全策略与程序不断更新，这增加了对策略与程序频繁审核的可能性，并且员工可以从中找到任何与信息安全有关的问题和答案。

最后，使用社会工程学方法与策略进行的周期性渗透测试与安全评估应当暴露出培训或公司策略和程序的不足。对于之前使

用的任何欺骗渗透测试策略，应当告知员工有时候可能会进行这种测试。

## 怎样使用这些策略

本章中介绍的详细策略是我认为对减轻所有安全威胁非常重要的信息安全策略子集，因此，这些策略并不是一个完整的列表，更确切的说，它们是创建合适的安全策略的基础。

企业的策略书写者可以基于他们公司的独特环境和商业目的选择适合的策略。每一家有不同安全需求（基于商业需要、法律规定、企业文化和信息系统）的企业都能在这些介绍找到所需的策略，而忽略其它的内容。

每一种策略都会提供不同的安全等级选择。大部分员工都互相认识的小型公司不需要担心攻击者会通过电话冒充员工（当然攻击者还可以伪装成厂商）。同样，一家企业文化轻松休闲的公司可能会希望只用这些策略中的一部分来达到它的安全目标，虽然这样做会增加风险。

## 数据分类

数据分类策略是保护企业信息资产、管理敏感信息存取的基础。这一策略能让所有员工了解每一种信息的敏感等级，从而提供了保护企业信息的框架。

没有数据分类策略的操作——几乎所有公司的现状——使得的大部分的控制权掌握在少数员工手里。可想而知，员工的决定在很大程度上依赖于主观判断，而不是信息的敏感性、关键程度和价值。如果员工不了解被请求信息的潜在价值，他们可能会把它交到一名攻击者手里。

数据分类策略详细说明了信息的贵重程度。有了数据分类，员工就可以通过一套数据处理程序保护公司安全，避免因疏忽而泄漏敏感信息，这些程序降低了员工将敏感信息交给未授权者的可能性。

每一个员工都必须接受企业数据分类策略培训，包括那些并不经常使用计算机或企业通信系统的人。因为企业中的每一个人——包括清洁工、门卫、复印室职员、顾问和承包人，甚至是实习医生——都有可能访问敏感信息，任何人都能成为攻击的目标。

管理层必须指定一个信息所有者负责公司目前正在使用的任何信息，信息所有者的职责之一就是保护信息资产。通常，所有者负责确定基于信息保护需要的分类等级，周期性地评估分类等级，并在必要的时候对其进行修改，信息所有者可能还会负责指

定管理人员或其他人员来保护数据。

分类类别与定义

应当基于敏感程度将信息分成不同的分类等级。一旦建立了详细的分类系统，重新分类信息将十分昂贵和费时。在我们的策略范例中，我选择了4个适合几乎所有大中型企业的分类等级。依靠敏感信息的编号和分类，商业公司可以选择增加更多分类以适应将来的特殊类型。在小型商业公司，三个等级的分类方案可能就够了。记住——分类方案越复杂，企业培训员工和执行方案的费用就越高。

机密是最敏感的信息分类，机密信息只能在企业内部使用。在大多数情况下，机密信息只能让少数有必要知道的人访问。机密信息的泄漏会严重影响到公司（股东、商业伙伴和（或）客户）。机密信息通常包括以下内容：

商业机密信息、私有源代码、技术或规格说明书、能被竞争者利用的产品信息。

并不公开的销售和财政信息。

关系到公司运转的其它任何信息，比如商业战略前景。

私有是仅在企业内部使用的个人信息分类。如果未授权的人（尤其是社会工程师）获得了私有信息，员工和公司都将受到严重影响。私有信息内容包括：员工病历、健康补助、银行帐户、加薪历史，和其它任何没有公共存档的个人识别信息。

注释：

内部信息分类通常由安全人员设定，我使用了“内部”这个词，因为这是分类使用的范围。我列出的这些敏感分类并不是详细的安全等级，而是查阅机密、私有和内部信息的快捷方式，用另一句话说，敏感程度涉及到了任何没有指定为公共权限的公司信息。

内部信息分类能提供给任何受雇于企业的员工。通常，内部信息的泄漏不会对公司（股东、商业伙伴、客户或员工）造成严重影响，但是，熟悉社会工程学技能的人能用这些信息伪装成一个已授权的员工、承包人或者厂商，从没有丝毫怀疑的员工那里获得更多敏感信息突破企业计算机系统的访问限制。

必须在传递内部信息给第三方（提供商、承包人、合作公司等等）之前与其签署一份保密协议。内部信息通常包括任何在日常工作中使用的、不能让外部人员知道的信息，比如企业机构

图、网络拨号号码、内部系统名、远程访问程序、核心代码成本、等等。

公共信息被明确规定为公共可用。这种信息类型，比如新闻稿、客服联系信息或者产品手册，能自由地提供给任何人。需要注意的是，任何为指定为公共可用的信息都应当视为敏感信息。

数据分类术语

上述内容的详细资料可以在第16章找到。

测试

你的公司可能需要在员工使用计算机系统之前测试他们是否已经掌握了这些安全知识。如果你想设计一个测试程序，有许多评价设计软件程序能让你轻松地分析测试的结果，锁定需要强化培训的范围。

你的公司可能会考虑提供一张证书作为奖励证明员工完成了安全培训。

作为完成程序的一部分，建议让每一个员工签署一份遵守安全策略和规定的同意书。调查报告显示，签署了同意书的人会更加严格地遵守程序。

持续的培训

如果不周期性的复习，大部分人会把学到的知识（甚至重要的事件）忘掉。为了不让员工忘记如何防范社会工程学攻击，持续的培训程序非常重要。

一种让员工记忆深刻的方法是把安全作为他们特殊的工作职责，这能让员工认为他们在公司安全体系内扮演着至关重要的角色，否则员工会强烈地倾向于安全"不是我的工作"。

当安全部门或信息技术部门的人承担了一个信息安全程序全部的职责时，信息安全培训程序最好的结构是与培训部门协同合作。

持续的培训程序需要创造性地使用所有可能的频道传输安全讯息，因为记忆的可存储性，员工们会不时地想起好的安全习惯。除了使用所有传统的频道之外，还要加上许多能够想到的非传统方式，就像传统的广告一样，幽默、灵活地提供帮助。灵活多变的讯息可以让员工更加熟悉安全策略而无法忽视。

持续的培训程序可能包括以下内容：

提供本书的复印件给所有员工。

在公司的新闻通讯中添加以下内容：文档，封装的提示（简短、引人注目的内容），比如漫画。

张贴当月的安全员工照片。

在员工区域张贴海报。

张贴公告牌通知。

为支票信封提供打印的外壳。

发送email提示。

使用安全相关的屏幕保护程序。

通过语音信箱系统广播安全提示。

打印电话贴纸，"你的呼叫者是他所声称的那个人吗？"

设置电脑登录时的提示信息，比如"如果你要发送机密信息到email，把它加密。"

把安全知识作为员工财政报告和年度评价的标准内容。

在intranet（企业内网）上提供安全知识提示，可以使用漫画或者幽默文字，或者其它能吸引员工阅读的方式。

在自助餐厅使用电子讯息显示板，频繁地更换安全提示。

分发传单或小册子。

还有一些小花招，比如在自助餐厅提供带有安全提示的免费饼干。

威胁总是存在，安全提示最好也总是存在。

"我能得到什么？"

除了安全知识与培训程序之外，我强烈推荐宣传并推行奖励程序。你必须答谢成功阻止了社会工程学攻击、或者在其它方面对信息安全程序作出了杰出贡献的员工。应当在所有培训课程上告知员工奖励程序的存在，并在企业范围内公布违反安全规定的人的名单。

从另一方面讲，人们必须认识到遵守信息安全策略的重要性是无法忽视或反抗的。虽然我们都会犯错误，但是重复的违反安全规定是不能容忍的。

基于其分类，数据应当由不同的人负责。本章中的许多策略都提到过不允许身份未验证的人访问信息，在这些策略中，未验证的人指的是员工并不亲自认识的人和不能确定是否有访问权限的员工，还有无法保证可信的第三方。

在这些策略中，可信的人是指你亲自见过的、有访问权限的公司员工、客户或者顾问，也可以是与你的公司有合作关系的人（比如，客户、厂商或者签署了保密协议的战略合作伙伴）。

在第三方的保证中，可信的人可以验证一个人的职业或身份，和这个人请求信息或操作的权限。注意，在某些情况下，这些策略会要求你在响应信息或操作请求之前确认保证者仍然受雇于公司。

特权帐户是指需要超越基本用户帐户权限的计算机（或其

它）帐户，比如系统管理员帐户。有特权帐户的员工通常能更改用户权限或执行系统操作。

常规部门信箱是指回答一般问题的语音信箱，用来保护在特殊部门工作的员工的名字和分机号码。

验证与授权程序

信息窃贼通常会伪装成合法的员工、承包人、厂商或商业伙伴，使用欺骗策略访问机密商业信息。为了保护信息安全，员工在接受操作请求或提供敏感信息之前，必须确认呼叫者的身份并验证他的权限。

本章中推荐的程序能帮助一名收到请求（通过任何通讯方式，比如电话、email或传真）的员工判断其是否合法。

可信者的请求

针对可信者的信息或操作请求：

确认其是否当前受雇于公司或者有权访问这一信息分类，这能阻止离职员工、厂商、承包人、和其他不再与公司有关系的人冒充可信的职员。

验证此人是否有权访问信息或请求操作。

未核实者的请求

当遇到未核实者的请求时，必须使用一个合理的验证程序确认请求者是否有权接收请求的信息，尤其是当请求涉及到任何计算机或计算机相关的设备时。这一程序成功防范社会工程学攻击的关键：只要实施了这些验证程序，社会工程学攻击成功的可能性将大大减小。

需要注意的是，如果你把程序设置得过于复杂，将超过成本限制并被员工忽略。

下面列出了详细的验证程序步骤：

验证请求者是他（或她）所声称的那个人。

确认请求者当前受雇于公司或者与公司有须知关系。

确认请求者已被授权接收指定信息或请求操作。

第一步：验证身份

以下列出的推荐步骤按有效性从低到高排列，每一条中还加入了社会工程师行骗的详细说明。

1、来电显示（假设这一功能已经包括在了公司的电话系统之中）。用来电显示确认电话是来自公司内部还是公司外部，显示

的名字和电话号码是否符合呼叫者提供的身份。

弱点：外部来电显示信息可以被任何能用PBX或者电话交换机连接到数字电话服务的人伪造。

2、回拨。在公司的目录中查询请求者的名字，并通过列出的分机号码回拨确认请求者的身份。

弱点：当员工回拨电话时，准备充分的攻击者可以将其呼叫转移到一个外部的电话号码。

3、担保。由一个可信的人为请求者的身份担保。

弱点：攻击者可以伪装成一个可信员工，让另一个员工为他担保。

4、接头暗号。在企业范围内使用接头暗号，比如每日密码。

弱点：如果有很多人知道这个接头暗号，攻击者也可以轻易地知道。

5、员工管理员/经理。打电话给员工的顶头上司并请求验证。

弱点：如果请求者提供了他（或她）的上司的电话号码，员工联系上的也许是攻击者的同谋。

6、安全Email。请求数字签名信息。

弱点：如果攻击者入侵了员工的计算机并通过键盘记录程序获取了密码，他便可以像普通员工一样发送数字签名email。

7、个人语音识别。通过声音判断请求者的身份。

弱点：这是相当安全的方法，攻击者无法轻易突破，但是如果没有见过请求者（或者和请求者说过话），这一方法就没有任何用处。

8、动态密码方案。请求者通过一个动态的密码方案（比如安全ID）识别自身。

弱点：攻击者可以获取其中的动态密码设备和相应的员工PIN码，或者欺骗员工读出PIN设备上显示的信息。

9、佩戴ID。请求者佩戴员工证件或其它合适的照片ID。

弱点：攻击者可以偷窃员工证件，或者直接伪造一张。然而，攻击者通常会避免这样做，以减小被发现的可能性。

第二步：验证员工身份

最大的信息安全威胁并不是专业的社会工程师，也不是熟练的计算机入侵者，而是刚刚解雇想要报复或者偷窃公司商业信息的员工。（注意，这一步骤的另一个版本可用于和你的公司有另一种商业关系的人，比如厂商、顾问或契约工人）

在提供敏感信息给另一个人或者接受计算机或计算机相关的设备指示操作之前，使用下面这些方法验证请求者是否仍是公司的员工：

查看员工目录。如果公司有一份活动员工目录，可以查看请求者是否仍在列表中。

请求者的上司核对。用公司目录上列出的电话号码打电话给请求者的上司，而不是使用请求者提供的号码。

请求者的部门或工作组验证。打电话给请求者的部门或工作组，从该部门或工作组的任何人那里确认请求者仍是公司的员工。

第三步：验证权限

除了验证请求者是否为活动员工或者与公司有关联之外，仍然有必要确认确认请求者已被授权访问所请求的信息，或者已被授权指导指定的计算机或计算机相关的设备操作。

可以使用以下这些方法进行验证：

职位/工作组/职责列表。企业可以使用一张列表说明指定的员工可以访问哪些指定信息，并通过员工的职位、部门、工作组、职责或者综合这些进行分类。这一列表需要不断更新并提供授权信息的快捷访问方式。通常，信息所有者应当负责创建并维护这一列表，监控信息的访问。

注释

值得注意的是，维护这种列表是在邀请社会工程师，试想一下，如果攻击者将一家公司作为目标，就会知道这一列表的存在，并有足够的兴趣获取一份，这一列表能为攻击者打开方便之门，使公司陷入严重的危机之中。

获得上司授权。员工联系他（或她）自己的上司，或者请求者的上司，请求授权同意这一请求。

获得信息所有者或指定人员的授权。信息所有者可以决定是否允许访问，基于计算机的访问控制程序可以让员工联系他（或她）的顶头上司申请访问基于工作任务的信息，如果这一任务不存在，管理人员有责任联系相关的数据所有者请求许可。这一管理系统的实施应当保证信息所有者不会拒绝常用信息的请求。

获得专业软件程序授权。对于高竞争性产业的大公司，可以使用专业软件程序进行授权。这种软件的数据库中存储了员工的姓名和机密信息访问权限，用户无法查看每个人的访问权限，但可以输入请求者的名字，并找到相关的权限信息。这种软件提供了响应标志，可以判断员工是否已被授权访问这一信息，并用独立的权限信息消除了创建个人列表的危险性。